AUTHORIZED DOCUMENTATION

Ajuda do Console de Gerenciamento

August 1, 2008

Novell®
ZENworks Endpoint Security Management

3.5

www.novell.com

Informações Legais

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Documentação Online: Para acessar a documentação online mais recente para este e outros produtos da Novell, consulte a página de Documentação da Novell (http://www.novell.com/documentation).

Índice

Utilizando o Console de Gerenciamento do ZENworks Endpoint Security

1

O Console de Gerenciamento é o acesso e o controle central do Serviço de Gerenciamento do Novell® ZENworks® Endpoint Security.

Para iniciar a janela de login do Console de Gerenciamento, clique em *Iniciar* > *Todos os Programas* > *Novell* > *Console de Gerenciamento do ESM* > *Console de Gerenciamento*. Para efetuar login no Console, especifique o nome e a senha do administrador. O nome de usuário digitado precisa ser o nome de um usuário autorizado no Serviço de Gerenciamento (consulte Seção 1.3, "Usando Configurações de Permissão" na página 10).

Observa o: Recomendamos que você feche ou minimize o console quando ele não estiver sendo usado.

1.1 Utilizando a barra de tarefas

A barra de tarefas localizada à esquerda fornece acesso às tarefas do Console de Gerenciamento. Se a barra de tarefas não estiver visível, clique no botão *Tarefas* à esquerda do console.

As seguintes seções contêm mais informações sobre as tarefas que podem ser realizadas com a barra de tarefas:

- Seção 1.1.1, "Tarefas de política" na página 8
- Seção 1.1.2, "Recursos" na página 8
- Seção 1.1.3, "Configuração" na página 8
- Seção 1.1.4, "Auditoria de Ponto de Extremidade" na página 9

1.1.1 Tarefas de política

A principal função do Console de Gerenciamento é criar e aplicar políticas de segurança a dispositivos gerenciados de ponto de extremidade. As tarefas de política orientam o administrador na criação e na edição de políticas de segurança que são usadas pelo ZENworks® Security Client para aplicar segurança gerenciada centralmente a cada dispositivo de ponto de extremidade.

As tarefas de política incluem o seguinte:

- **Políticas Ativas:** Exibe uma lista das políticas que podem ser analisadas e editadas no momento. Clique em uma política para abri-la.
- **Criar Política:** Inicia o Assistente de Nova Política, que permite criar uma nova política de segurança.
- **Importar Política:** Exibe a caixa de diálogo Importar Política, que permite importar políticas criadas com outros serviços de gerenciamento. Para obter mais informações, consulte Seção 2.3.1, "Importando políticas" na página 107.

Se você clicar em uma das tarefas de política, a barra de tarefas será minimizada. Clique no botão *Tarefas* à esquerda para reabri-la.

Consulte Capítulo 2, "Criando e distribuindo políticas de segurança" na página 45 para aprender mais sobre tarefas de política e sobre como criar e gerenciar políticas de segurança.

1.1.2 Recursos

A lista de tarefas Recursos exibe os recursos de suporte técnico e ajuda disponíveis:

- **Contatar Suporte:** Inicia um browser e exibe a página Contatos e escritórios da Novell®.
- **Suporte Técnico Online:** Inicia um browser e exibe a página Treinamento e suporte da Novell.
- **Ajuda do Console de Gerenciamento:** Inicia a Ajuda online do ZENworks® Endpoint Security Management.

1.1.3 Configuração

A janela Configuração do Serviço de Gerenciamento contém controles para a infra-estrutura do servidor ZENworks® Endpoint Security Management e para o monitoramento de serviços de diretório adicionais da empresa. Para obter mais informações, consulte Seção 1.4, "Utilizando a janela Configuração" na página 14. Esse controle não está disponível quando o Console de Gerenciamento Independente é executado. Para obter mais informações, consulte o *Guia de Instalação do ZENworks Endpoint Security Management*.

1.1.4 Auditoria de Ponto de Extremidade

A janela Auditoria de Ponto de Extremidade fornece acesso aos recursos de alertas e de geração de relatórios do ZENworks® Endpoint Security Management.

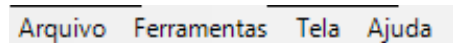
Gerador de Relatórios: A geração de relatórios é importante para a avaliação e a implementação de políticas de segurança avançadas. Para acessar os relatórios, no Console de Gerenciamento, clique em *Relatórios*. As informações de segurança de pontos de extremidade reunidas e relatadas também são completamente configuráveis e podem ser reunidas por domínio, grupo ou usuário individual. Para obter mais informações, consulte Seção 1.6, “Utilizando o gerador de relatórios” na página 28.

Alertas: O monitoramento de alertas assegura que quaisquer tentativas de comprometer as políticas de segurança sejam relatadas no Console de Gerenciamento. Os alertas informam ao administrador do ZENworks Endpoint Security Management sobre possíveis problemas e permitem que o administrador execute as ações de remediação apropriadas. O painel Alertas é completamente configurável; portanto, você tem total controle para decidir quando e com que freqüência os alertas serão acionados. Para obter mais informações, consulte Seção 1.5, “Utilizando monitoramento de alertas” na página 24.

1.2 Utilizando a barra de menus

A barra de menus do ZENworks® Endpoint Security Management fornece acesso a todas as funções do Console de Gerenciamento

As seguintes opções estão disponíveis:

Arquivo Ferramentas Tela Ajuda

- **Arquivo:** Use o menu Arquivo para criar e gerenciar políticas de segurança.
    - **Criar Nova Política:** Inicia o Assistente de Nova Política, que permite criar uma nova política de segurança.
    - **Atualizar Lista de Políticas:** Atualiza a lista de políticas para exibir todas as políticas ativas.
    - **Apagar Política:** Apaga a política selecionada.
    - **Importar Política:** Permite importar uma política para o Console de Gerenciamento.
    - **Exportar Política:** Permite exportar uma política e o arquivo `setup.sen` necessário para um local especificado fora do banco de dados do Serviço de Gerenciamento.
    - **Sair:** Fecha o software Console de Gerenciamento e efetua o logout do usuário.
- **Ferramentas:** Use o menu Ferramentas para controlar a configuração, as chaves criptográficas e as permissões do Serviço de Gerenciamento.
    - **Configuração:** Abre a janela Configuração.
    - **Exportar Chaves Criptográficas:** Abre a caixa de diálogo Exportar Chaves Criptográficas, onde você especifica as chaves a serem exportadas e a senha.
    - **Importar Chaves Criptográficas:** Abre a caixa de diálogo Importar Chaves Criptográficas, onde você especifica as chaves a serem importadas e a senha.

- **Gerar Nova Chave:** Gera uma nova chave criptográfica para assegurar a proteção dos dados.
- **Permissões:** Abre a janela Permissões.

- **Ver:** Use o menu Ver para executar as principais tarefas de política sem utilizar a barra de tarefas.
  - **Política:** Quando uma política é aberta, essa opção alterna a tela para essa política.
  - **Políticas Ativas:** Exibe a lista de políticas.
  - **Alertas:** Exibe o painel Alertas.
  - **Gerador de Relatórios:** Exibe o painel Gerador de Relatórios.
- **Ajuda:** Exibe a ferramenta Ajuda do Console de Gerenciamento e a caixa de diálogo Sobre:
  - **Ajuda:** Inicia a Ajuda online do Console de Gerenciamento, que orienta você na criação de uma política e em todas as tarefas do Console de Gerenciamento. Você também pode acessar a Ajuda pressionando a tecla F1 no teclado.
  - **Sobre o Console de Gerenciamento:** Abre a janela Sobre, que exibe o tipo de instalação (ZENworks Endpoint Security Management ou UWS) e o número da versão atual do Console de Gerenciamento. É nessa janela também que a chave de licença será digitada se for adquirida após a instalação.

1.3 Usando Configurações de Permissão

A opção Configurações de Permissão está localizada no menu Ferramentas e só pode ser acessada pelo administrador principal do Serviço de Gerenciamento ou por qualquer pessoa que tenha recebido desse administrador acesso permissões. Esse controle não está disponível quando o Console de Gerenciamento Independente é executado.

As configurações de permissão definem que usuários ou grupos de usuários terão permissão para acessar o Console de Gerenciamento, as Permissões Administrativas ou as configurações de Publicar Para.

Durante a instalação do Servidor de Gerenciamento, é inserido no formulário de configuração um nome de administrador ou Conta de Recurso para o usuário do recurso (consulte o *Guia de Instalação do ZENworks Endpoint Security Management*). Depois que um teste for executado e que as informações do usuário forem gravadas, todas as permissões serão automaticamente concedidas a esse usuário.

Após a instalação do Console de Gerenciamento, o usuário do recurso será o único usuário com todas as permissões, embora todos os grupos de usuários do domínio tenham acesso ao Console de Gerenciamento. O usuário do recurso deverá impedir o acesso de todos os grupos ou usuários que não tiverem permissão. O usuário do recurso pode definir permissões adicionais para os usuários designados.

Quando o Console de Gerenciamento é iniciado, as permissões são recuperadas da tabela Permissão. Essas permissões informam ao console se o usuário possui direitos para efetuar login no Console, para criar ou apagar políticas, para mudar configurações de permissão, e também se ele pode ou não publicar políticas e para quem eles pode publicá-las.

As seguintes configurações de acesso estão disponíveis:

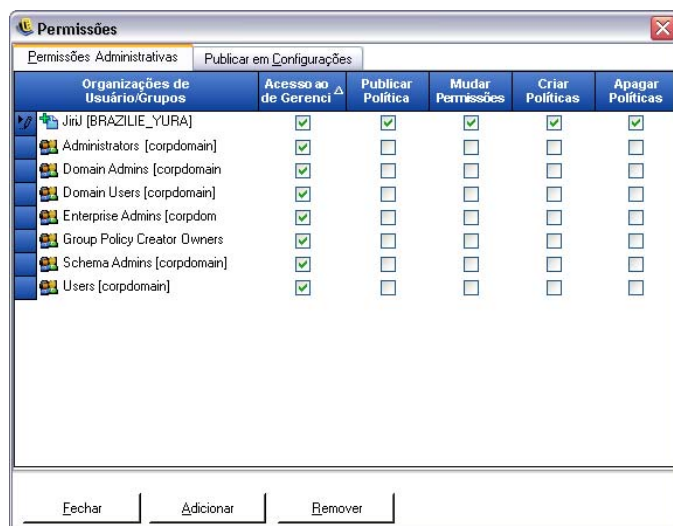
- **Acesso ao Console de Gerenciamento:** O usuário pode ver políticas e componentes, e também editar políticas existentes. Os usuários com apenas esse privilégio concedido não terão permissão para adicionar ou apagar políticas; as opções de publicação e permissão não estarão disponíveis.
- **Publicar Política:** O usuário só pode publicar políticas para usuários ou grupos designados.
- **Mudar Permissão:** O usuário pode acessar e mudar configurações de permissão de outros usuários já definidas ou conceder permissões a novos usuários.
- **Criar Políticas:** O usuário pode criar novas políticas no Console de Gerenciamento.
- **Apagar políticas:** O usuário pode apagar qualquer política do Console de Gerenciamento.

Observa o: Por motivos de segurança, é recomendável que somente o usuário do recurso ou alguns poucos administradores tenham as permissões Mudar Permissão e Apagar Políticas.

1.3.1 Permissões Administrativas

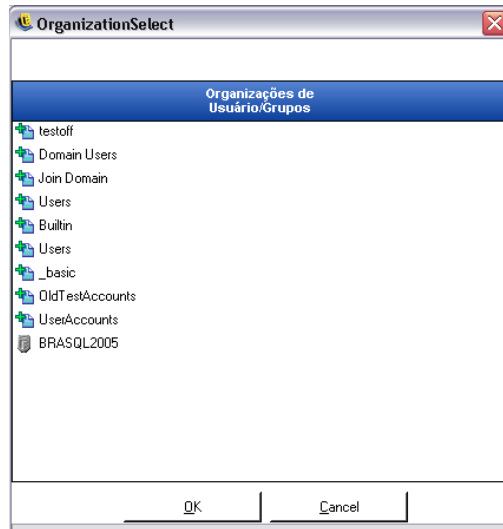
Para definir as permissões administrativas:

1 Clique em *Ferramentas* > *Permissões*.

Os grupos associados a este domínio são mostrados.

Observa o: Por padrão, todos os grupos recebem acesso ao Console de Gerenciamento, ainda que não possam realizar tarefas de política. Para remover o acesso ao console, desmarque a permissão.

---

2 Para carregar esta lista com usuários ou grupos:

2a Clique no botão *Adicionar* na parte inferior da tela.

2b Selecione os usuários ou os grupos apropriados na lista. Para selecionar vários usuários, selecione-os individualmente mantendo pressionada a tecla Ctrl, ou selecione uma série, marcando o primeiro, mantendo pressionada a tecla Shift e depois marcando o último.

2c Quando todos os usuários ou grupos tiverem sido selecionados, clique no botão *OK*.

3 Atribua qualquer permissão (ou todas as permissões) aos usuários ou grupos disponíveis.

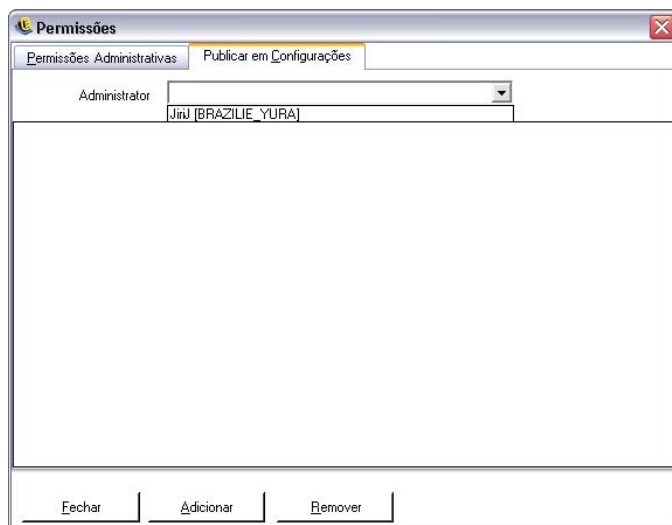
Para remover um usuário ou um grupo selecionado, marque o nome desejado e clique em *Remover*. O nome selecionado será movido de volta para a Tabela de Organização.

1.3.2 Configurações de Publicar Para

Usuários ou grupos de publicação deverão ser designados aos usuários ou grupos cuja opção *Publicar Política* estiver marcada.

Para definir Configurações de Publicar Para:

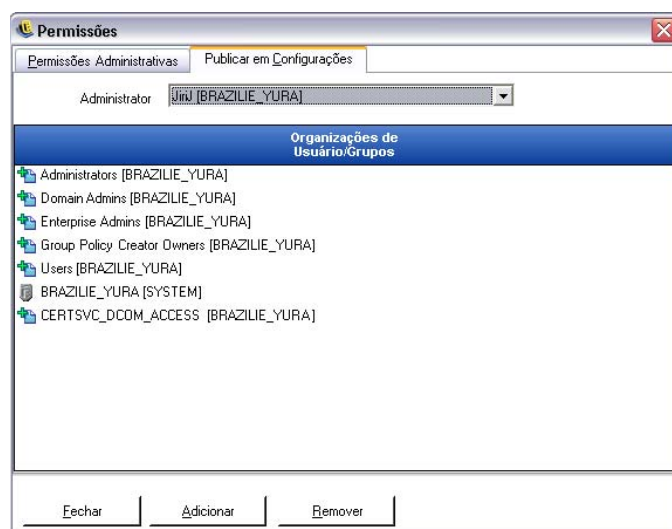
1 Clique na guia *Configurações de Publicar Para*.

2 Selecione na lista suspensa os usuários ou os grupos aos quais a permissão Publicar foi concedida.

3 Atribua usuários ou grupos a este usuário/grupo:

3a Clique no botão *Adicionar* na parte inferior da tela para exibir a Tabela de Organização.

3b Selecione os usuários ou os grupos apropriados na lista. Você pode usar as teclas Ctrl e Shift para selecionar vários usuários.

3c Depois que todos os usuários ou grupos tiverem sido selecionados, clique no botão *OK* para adicionar esses usuários ou grupos à lista de publicação

do nome selecionado.

As definições de permissão são implementadas imediatamente.

4 Para remover um usuário ou um grupo selecionado, marque o nome desejado na lista e clique em *Remover*.

5 Clique em *Fechar* para aceitar as mudanças e retornar ao editor.

O nome selecionado será movido de volta para a Tabela de Organização.

Se um novo serviço de diretório for adicionado (consulte “Autenticação de Diretórios” na página 16), a Conta de Recurso inserida terá configurações de permissões totais, conforme descrito anteriormente.

1.4 Utilizando a janela Configuração

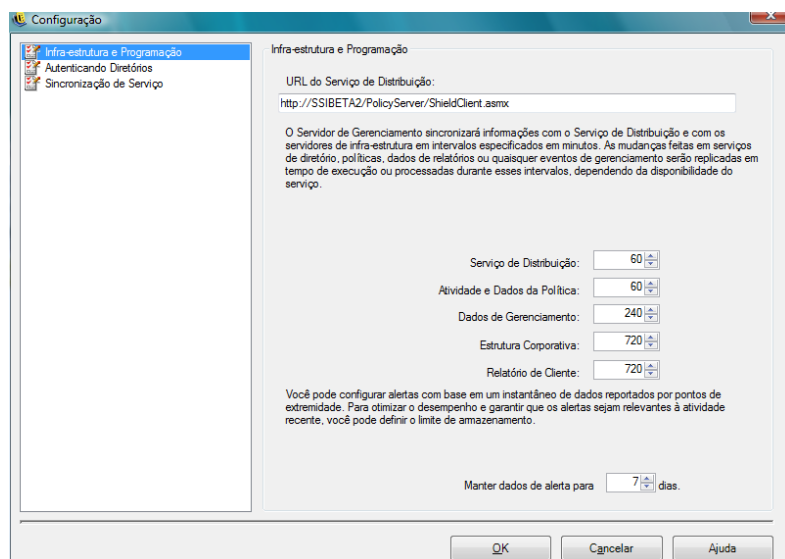
A janela Configuração permite ao administrador do ZENworks® Endpoint Security Management acessar os controles *Infra-estrutura e Programação*, *Diretórios de Autenticação* e *Sincronização do Servidor*. Na página principal, clique no link *Configuração*. Outra alternativa é clicar no menu *Ferramentas* e, em seguida, clicar em *Configuração*. A janela Configuração é exibida.

Observa o: Esse recurso não está disponível com o Console de Gerenciamento Independente.

As seções a seguir contêm mais informações:

- Seção 1.4.1, “Infra-estrutura e Programação” na página 14
- Seção 1.4.2, “Autenticação de Diretórios” na página 16
- Seção 1.4.3, “Sincronização de Serviços” na página 23

1.4.1 Infra-estrutura e Programação

O módulo de infra-estrutura e programação permite ao administrador do ZENworks Endpoint Security Management indicar e mudar o URL do Serviço de Distribuição de Políticas e controlar os intervalos de sincronização dos componentes do ZENworks Endpoint Security Management.

As seções a seguir contêm mais informações:

- “URL do Serviço de Distribuição” na página 15
- “Programação” na página 15

URL do Serviço de Distribuição

A configuração do *URL do Serviço de Distribuição* atualizará a localização do Serviço de Distribuição de Políticas do Serviço de Gerenciamento e de todos os ZENworks Security Clients (sem exigir que eles sejam reinstalados) se o Serviço de Distribuição de Políticas for movido para um novo servidor. O URL do servidor atual é listado no campo de texto.

Se precisar mudar o servidor, mude apenas o nome do servidor para apontar para o novo servidor. Não mude nenhuma informação de acordo com o nome do servidor.

Por exemplo, se o URL atual estiver listado como `http:\\ACME\PolicyServer\ShieldClient.asmx` e o Serviço de Distribuição de Políticas for instalado em um novo servidor chamado ACME 43, o URL deverá ser atualizado para `http:\\ACME43\PolicyServer\ShieldClient.asmx`.

Após atualizar o URL, clique em *OK* para atualizar todas as políticas e enviar uma atualização automática do Serviço de Distribuição de Políticas. Esse procedimento também atualizará o Serviço de Gerenciamento.

Quando mudar o URL do servidor, só encerre o Serviço de Distribuição de Políticas antigo quando as políticas atualizadas apresentarem um nível de aderência de 100% (consulte Seção 1.6, “Utilizando o gerador de relatórios” na página 28).

Programação

Os componentes de Programação permitem ao Administrador do ZENworks Endpoint Security Management indicar quando o Serviço de Gerenciamento será sincronizado com outros componentes do ZENworks Endpoint Security Management, para garantir que todos os dados e tarefas em fila correspondam às atividades recentes e para programar as tarefas de manutenção de SQL. Todos os incrementos de tempo estão em minutos.

A programação é dividida da seguinte forma:

- **Serviço de Distribuição:** Programação de sincronização com o Serviço de Distribuição de Políticas.
- **Dados e Atividade da Política:** Programação de sincronização com atualizações de política.
- **Dados de Gerenciamento:** Sincronização de políticas com o Serviço de Gerenciamento.
- **Estrutura do Empreendimento:** Programação de sincronização com o serviço de diretórios do empreendimento (eDirectory™, Active Directory*, NT Domain* e/ou LDAP). Mudanças no serviço de diretório do empreendimento são monitoradas para que as mudanças correspondentes nas designações de políticas do usuário sejam detectadas e enviadas ao Serviço de Distribuição de Políticas para autenticação do cliente.
- **Gerador de Relatórios do Cliente:** Com que freqüência o Serviço de Gerenciamento faz pesquisas e downloads de dados de relatórios no Serviço de Distribuição de Políticas.
- **Manter dados de alerta para:** É possível configurar alertas com base em um instantâneo dos dados reportados pelos pontos de extremidade. Para otimizar o desempenho e garantir que os alertas sejam relevantes para a atividade recente, defina o limite de armazenamento com base em um número de dias.

1.4.2 Autenticação de Diretórios

Depois de instalar o ZENworks® Endpoint Security Management, você deverá criar e configurar um serviço de diretório antes de começar a gerenciar dispositivos no sistema.

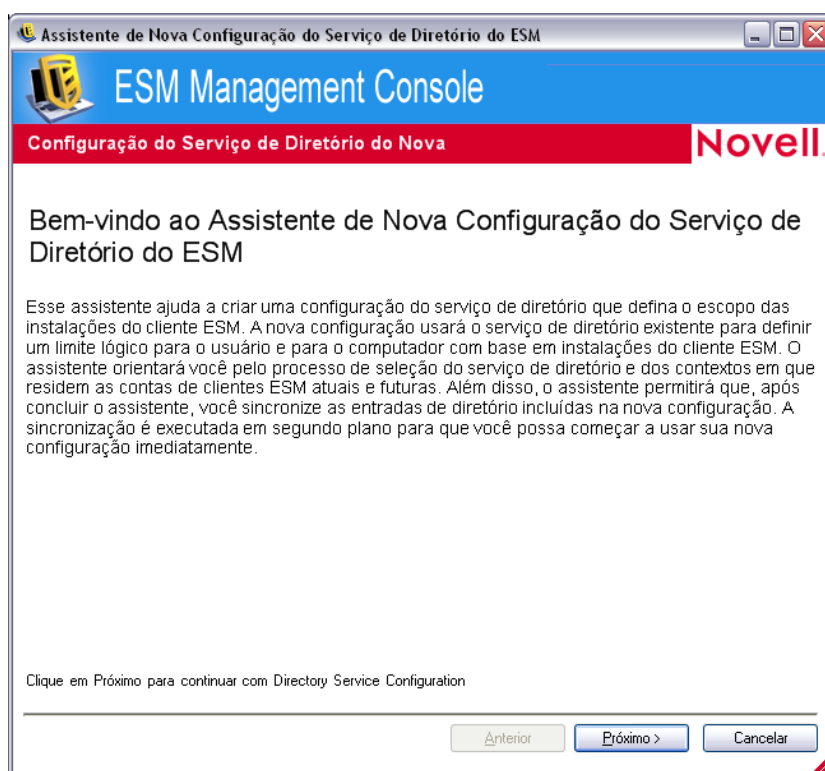
O Assistente de Nova Configuração do Serviço de Diretório permite criar uma configuração do serviço diretório que defina o escopo das instalações do seu cliente do ZENworks Endpoint Security Management. A nova configuração usa o serviço de diretório existente para definir a divisa lógica das instalações de cliente baseadas em usuário e em computador.

O assistente orienta você através do processo de seleção do serviço de diretório e dos contextos em que residem as contas de cliente atuais e futuras.

Além disso, o assistente permite sincronizar as entradas de diretório incluídas na nova configuração. Essa sincronização é executada em segundo plano para que você possa começar a usar imediatamente sua nova configuração.

Depois que você instalar o ZENworks Endpoint Security Management, o Assistente de Nova Configuração do Serviço de Diretório será exibido automaticamente. Se você tiver acabado de instalar o produto e a página de boas-vindas for exibida, vá para Etapa 4 no procedimento seguinte.

Para configurar o serviço de diretório:

1. No Console de Gerenciamento, clique em *Ferramentas* > *Configuração*.
2. Clique em *Diretórios de Autenticação*.
3. Clique em *Novo* para iniciar o Assistente de Nova Configuração do Serviço de Diretório.

4. Clique em *Avançar* para exibir a página Configurar Servidor.

5 Preencha os campos:

- **Tipo de Serviço:** Selecione um tipo de serviço na lista suspensa *Tipo de Serviço*:
  - Microsoft Active Directory
  - Novell eDirectory
- **Nome:** Especifique um nome amigável para descrever a configuração do serviço de diretório.
- **Nome do Host:** Especifique ou procure o nome DNS ou o endereço IP do servidor de diretórios.
- **Porta:** Especifique a porta usada na conexão com o servidor de diretórios.

  O padrão é a porta 389. Se usar outra porta para estabelecer conexão com o servidor de diretórios, especifique-a.

6 Clique em *Avançar* para exibir a página Fornecer Credenciais.

7 Preencha os campos:

- **Nome do Usuário:** Especifique o administrador de conta a ser vinculado ao diretório.

  Essa conta atua como o administrador da configuração de serviço de diretório. O nome de login digitado deve ser um usuário que tenha permissão para ver toda a árvore de diretório. Recomenda-se que esse usuário seja o administrador do domínio ou um administrador da OU. Se estiver configurando para o eDirectory, use um formato LDAP, como `cn=admin,o=acmeserver`, onde `cn` é o usuário e `o` é o objeto em que a conta de usuário está armazenada.

- **Senha:** Especifique a senha do administrador da conta.

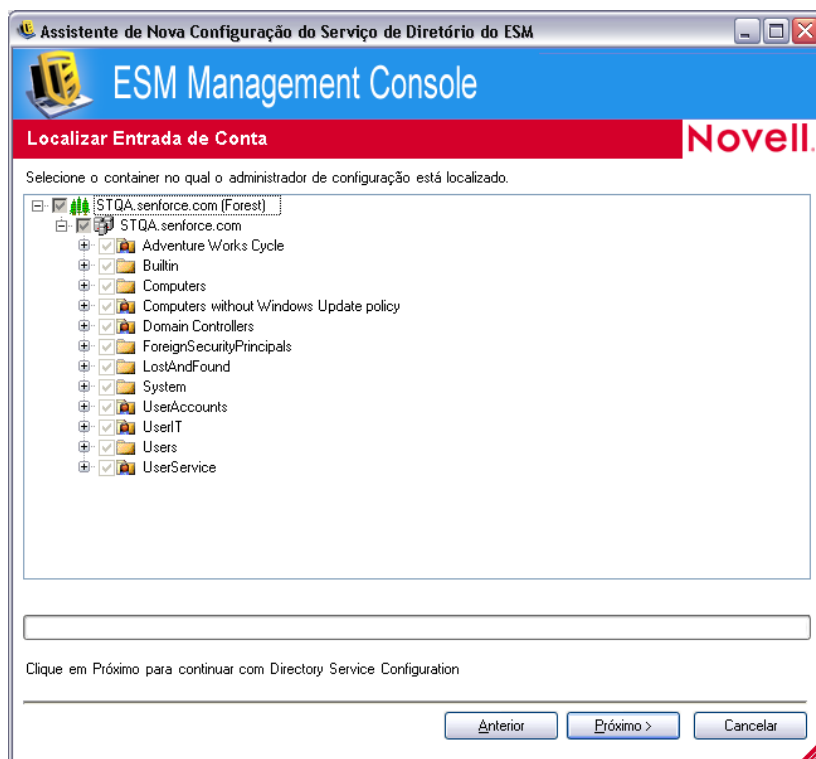
  Essa conta atua como o administrador da configuração do serviço de diretório.

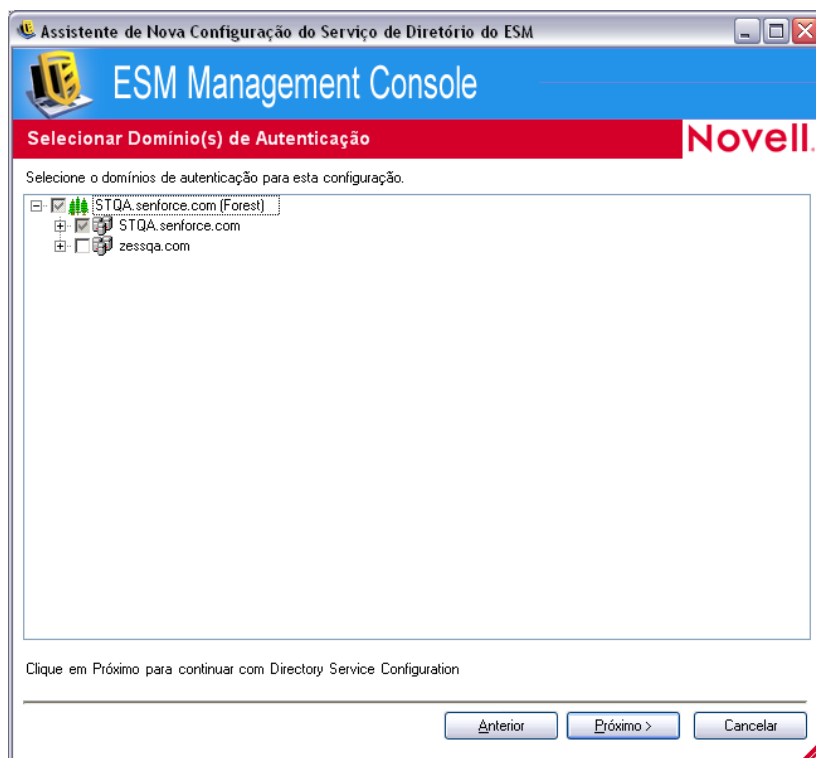
  A senha não deve ser definida para expirar e a conta nunca deve ser desabilitada.

- **Domínio:** Especifique o domínio do qual o administrador da conta é membro.

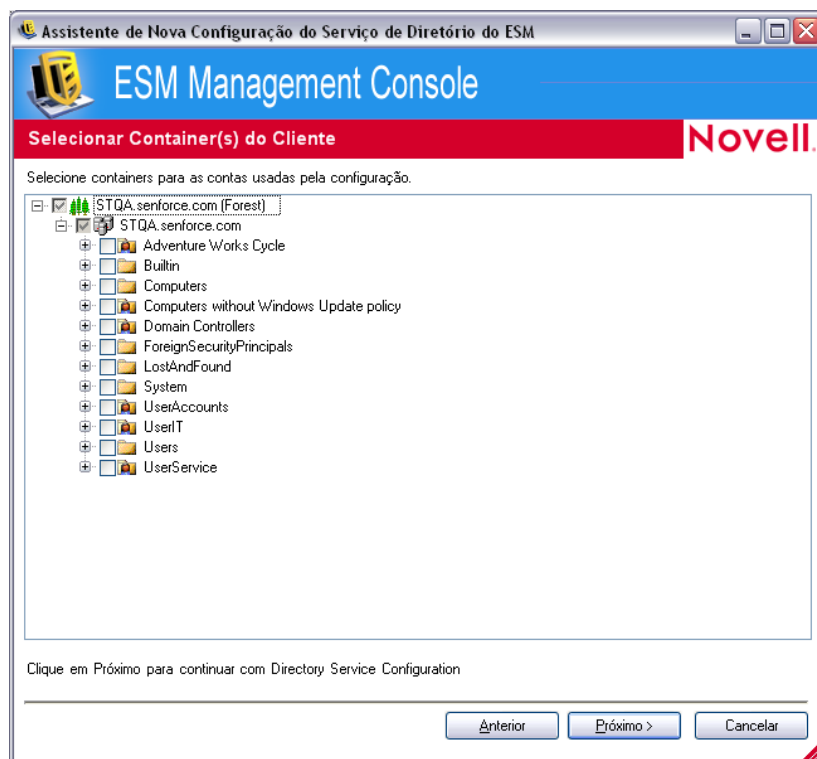
- **Estabeleça conexão com o servidor usando autenticação segura:** Anule a seleção dessa opção se não quiser usar autenticação segura. Essa opção está habilitada por padrão.

8 Clique em *Avançar* para continuar.

9 Se o administrador da configuração especificado em Etapa 7 não for encontrado no domínio, a página Localizar Entrada da Conta será exibida.

Especifique o container em que o administrador está localizado e clique em *Avançar*.

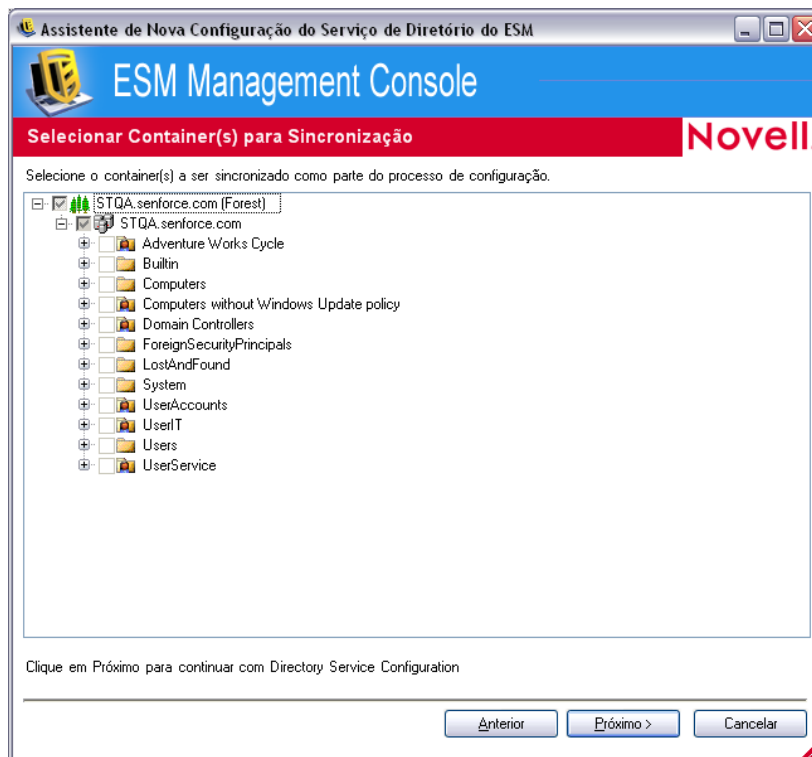
10 Na página Selecionar Domínios de Autenticação, procure e selecione na árvore os domínios usados para autenticar os usuários e os computadores dessa configuração.

O domínio que contém o usuário administrativo especificado em Etapa 7 é selecionado e sua seleção não pode ser anulada.

Qualquer instalação de cliente que tentar registrar entrada no servidor de gerenciamento falhará se não for membro de um dos domínios selecionados na configuração.

11 Clique em *Avançar* para exibir a página Selecionar Containers do Cliente e selecione os containers das contas usadas pela configuração.

O container que possui o usuário administrativo especificado em Etapa 7 é selecionado e sua seleção não pode ser anulada.

A página Selecionar Containers do Cliente permite restringir a pesquisa apenas aos containers que possuem usuários e computadores gerenciados, o que melhora o desempenho.

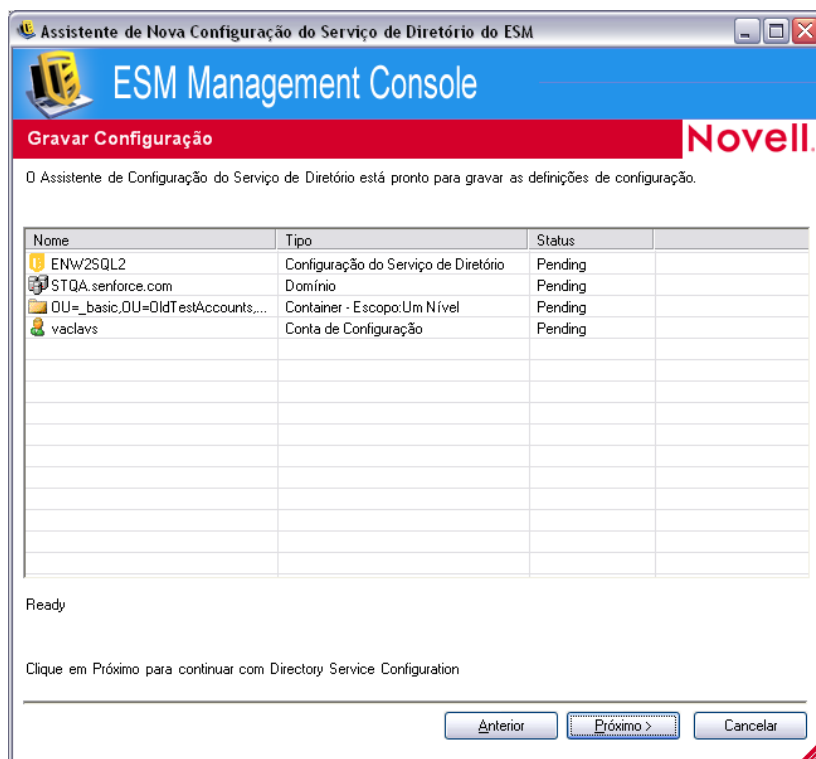
Qualquer instalação de cliente que tentar registrar entrada no servidor de gerenciamento falhará se sua conta não residir em um dos containers selecionados na configuração.

12 Clique em *Avançar* para exibir a página Containers para Sincronização.

13 (Opcional) Selecione os containers a serem sincronizados como parte do processo de configuração.

Essa sincronização é executada em segundo plano para que você possa começar a usar imediatamente sua nova configuração. Se houver muitos usuários e computadores a serem sincronizados, esse processo poderá levar algumas horas.

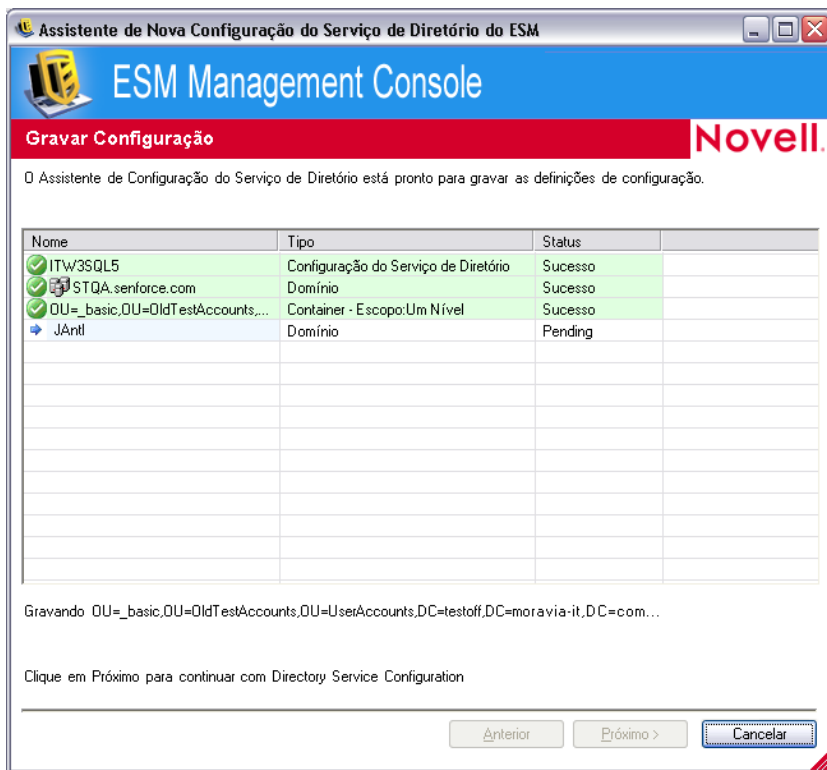
Se você não especificar containers para sincronização, o Console de Gerenciamento será preenchido com os usuários e os computadores contidos nos containers quando eles registrarem entrada.

A sincronização de containers preenche previamente o Console de Gerenciamento com os usuários e os computadores para que você possa executar ações, como criar políticas de segurança, imediatamente. Quando os usuários ou os computadores registram entrada no sistema, essas políticas são distribuídas e aplicadas. Ao preencher previamente o Console de Gerenciamento, você pode começar imediatamente a criar políticas específicas a usuários ou computadores individuais, em vez de criar uma política que se aplique a todos os usuários e computadores do container. Se não sincronizar o container, você precisará aguardar que os computadores e os usuários registrem entrada no sistema antes de criar políticas exclusivas para eles.

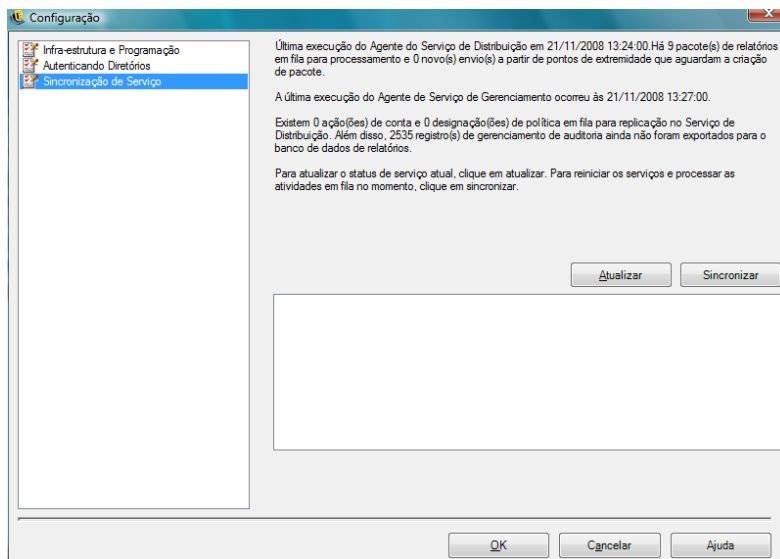
14 Clique em *Avançar* para exibir a página Gravar Configuração.

15 Analise as informações e clique em *Avançar* para gravar a configuração.

Se necessário, você poderá clicar em *Voltar* para mudar a configuração.

16 Clique em *Terminar*.

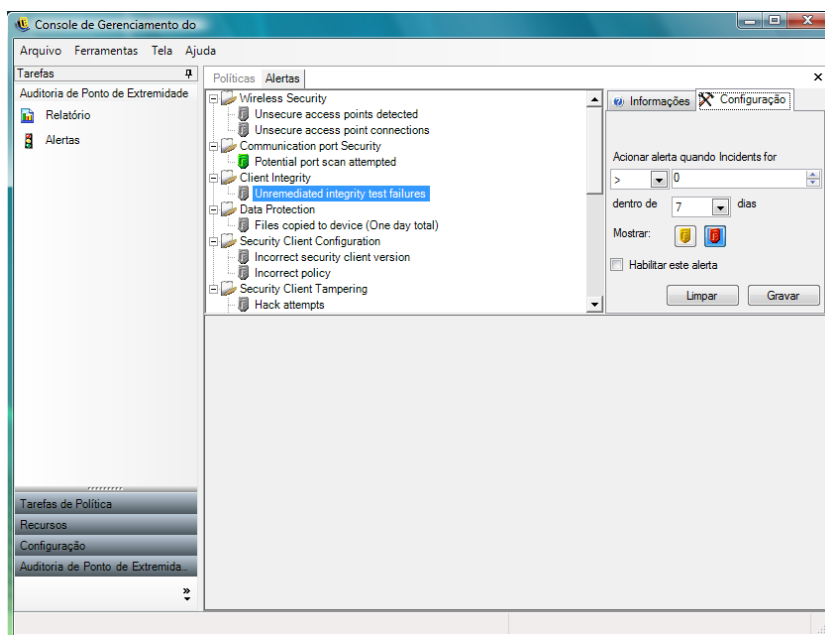
Quando você clica em *Terminar*, o ícone é exibido na área de notificação do Windows e a sincronização é iniciada. Clique duas vezes no ícone para exibir a caixa de diálogo Sincronização de Serviços de Diretório.

A sincronização será executada em segundo plano. Se você sair do Console de Gerenciamento, a sincronização será interrompida. Quando você abrir o Console de Gerenciamento novamente, a sincronização continuará do ponto em que parou.

1.4.3 Sincronização de Serviços

Esse controle permite forçar uma sincronização entre o Serviço de Gerenciamento e o Serviço de Distribuição de Políticas. Isso atualiza todos os alertas, relatórios e distribuições de políticas.

1. Para atualizar o status atual do serviço, clique em *Atualizar*.
2. Para reiniciar os serviços e processar as atividades atualmente em fila, clique em *Sincronizar*.

1.5 Utilizando monitoramento de alertas

O monitoramento de alertas permite que o administrador do ZENworks® Endpoint Security Management avalie o estado de segurança de todos os pontos de extremidade gerenciados do ZENworks Endpoint Security Management em toda a empresa. Os acionadores de alertas são totalmente configuráveis e podem reportar um aviso ou um alerta de emergência total. Para acessar essa ferramenta, use a *Auditoria de Ponto de Extremidade* na barra de tarefas ou o menu *Ver*.

1 Para acessar Alertas, clique no ícone Alertas (Alertas).

O monitoramento de alertas está disponível para as seguintes áreas:

- **Integridade de Clientes:** Notifica sobre os resultados dos testes de integridade não remediados.
- **Segurança de Portas de Comunicação:** Notifica sobre as possíveis tentativas de exploração de porta.
- **Proteção de Dados:** Notifica sobre os arquivos que são copiados para dispositivos de armazenamento removíveis no período de um dia.
- **Configuração de Cliente de Segurança:** Notifica sobre versões incorretas de clientes de segurança e sobre políticas incorretas.
- **Falsificação de Cliente de Segurança:** Notifica sobre tentativas de hacking, sobre tentativas de desinstalação e sobre a utilização da senha de anulação.
- **Segurança Sem Fio:** Notifica sobre pontos de acesso não seguros detectados ou conectados pelo usuário.

1.5.1 Configurando o ZENworks Endpoint Security Management para alertas

O monitoramento de alertas requer que os dados do gerador de relatórios sejam coletados e carregados em intervalos regulares para mostrar o quadro mais preciso do ambiente de segurança atual dos pontos de extremidade. Os ZENworks® Security Clients não gerenciados não fornecem dados do gerador de relatórios e, portanto, não são incluídos no monitoramento de alertas.

As seções a seguir contêm mais informações:

- "Ativando o gerador de relatórios" na página 25
- "Otimizando a sincronização" na página 25

Ativando o gerador de relatórios

O gerador de relatórios deve ser ativado em todas as políticas de segurança. Consulte Seção 2.2.4, "Gerador de Relatórios de Compatibilidade" na página 102 para obter detalhes sobre como configurar o gerador de relatórios para uma política de segurança. Ajuste o tempo de envio de relatórios para um intervalo que forneça atualizações consistentes sobre o status do ponto de extremidade. Além disso, nenhum alerta é ativado sem um relatório. Qualquer atividade sobre a qual você deseja ser alertado deve ter um relatório apropriado designado a ela na política de segurança.

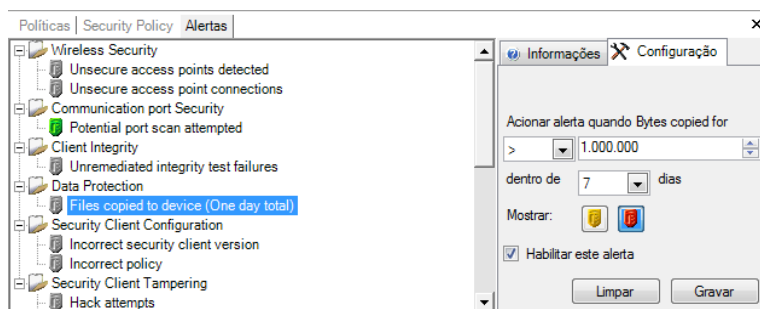
Otimizando a sincronização

Por padrão, o Serviço de Geração de Relatórios do ZENworks Endpoint Security Management é sincronizado a cada 12 horas. Isso significa que os dados iniciais de relatórios e alertas só estarão prontos 12 horas após a instalação do ZENworks Endpoint Security Management. Para ajustar esse período, abra a ferramenta Configuração (consulte "Programação" na página 15) e ajuste o tempo de *Gerador de Relatórios do Cliente* de acordo com o número de minutos adequado às suas necessidades e ao seu ambiente.

Quando há urgência na obtenção dos dados, a opção *Sincronização de Serviços* da ferramenta Configuração pode iniciar imediatamente o Serviço de Distribuição de Políticas (que coleta os dados do gerador de relatórios dos pontos de extremidade) e o Serviço de Geração de Relatórios (que atualiza todos os alertas com base nos novos dados coletados). Consulte Seção 1.4.3, "Sincronização de Serviços" na página 23 para obter detalhes.

1.5.2 Configurando acionadores de alertas

Os acionadores de alertas podem ser ajustados a limites que correspondam às suas necessidades de segurança corporativa.

1 Selecione um alerta na lista e clique na guia *Configuração* à direita do Console de Gerenciamento.

2 Para ajustar o limite do acionador, selecione a condição na lista suspensa. Isso define se o número do acionador é:

- Igual a (=)
- Maior que (<)
- Maior que ou igual a (<=)
- Menor que (>)
- Menor que ou igual a (>=)

3 Ajuste o número do acionador. Esse número varia de acordo com o tipo de alerta.

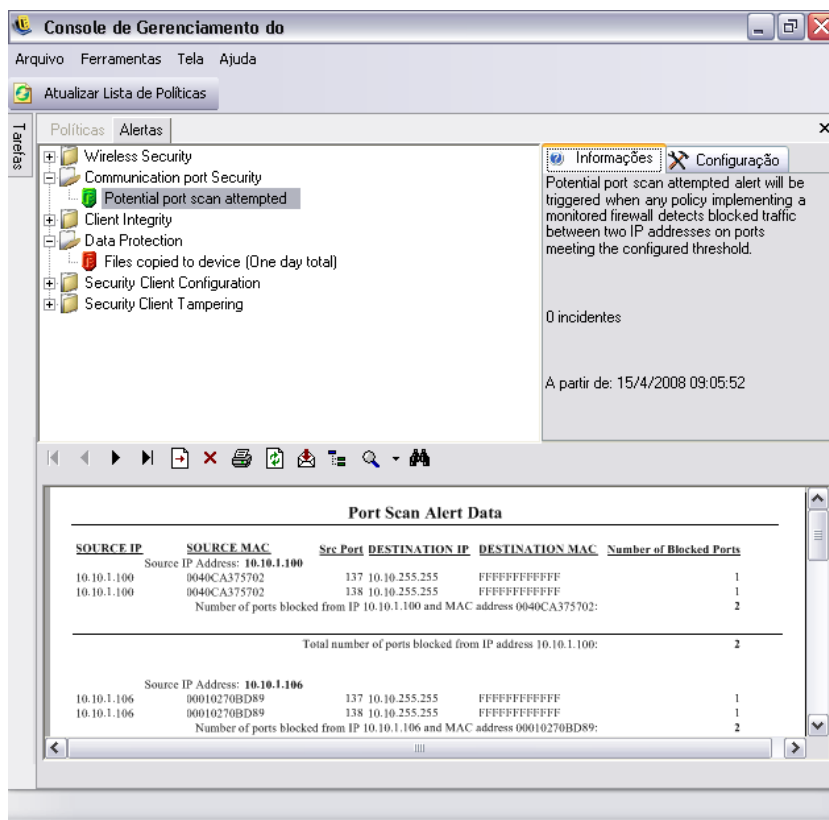
4 Selecione o intervalo no qual o número deve estar contido.

5 Selecione o tipo de acionador. Pode ser um ícone de aviso ( ) ou um ícone de emergência ( ).

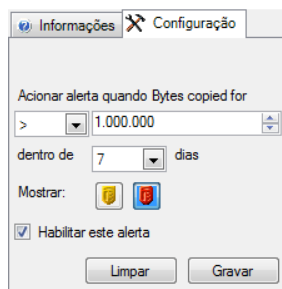
6 Verifique se a caixa *Habilitar Alerta* está marcada.

7 Clique em *Gravar* para gravar o alerta.

1.5.3 Gerenciando alertas

Os alertas notificam sobre problemas que precisam ser remediados dentro do ambiente de segurança dos pontos de extremidade. Geralmente, a remediação é realizada individualmente ou por grupo. Para ajudar a identificar o problema, os Relatórios de Alertas são exibidos quando o alerta é selecionado.

Esse relatório exibe os resultados atuais dos acionadores, mostrando informações sobre o usuário ou o dispositivo afetado. Os dados fornecidos aqui contêm as informações necessárias para a remediação de possíveis problemas de segurança corporativa. Para obter informações adicionais, abra o Gerador de Relatórios.

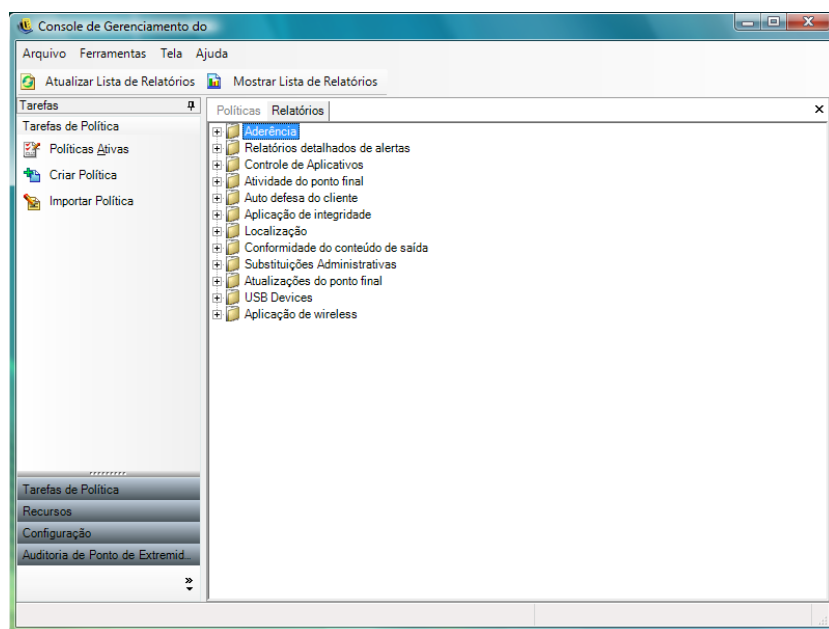
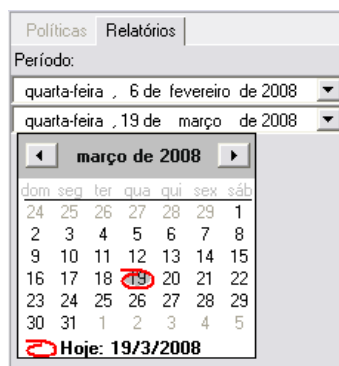
Depois que as ações de remediação tiverem sido executadas, o alerta permanecerá ativo até a próxima atualização de relatórios. Para limpar um alerta antes de uma atualização programada:

1. Selecione um alerta na lista e clique na guia *Configuração* à direita do Console de Gerenciamento.

2. Clique em *Limpar*.

   Isso limpará os dados do gerador de relatórios de Alertas (esses dados ainda estarão disponíveis no banco de dados do gerador de relatórios). A reativação ocorrerá quando novos dados forem recebidos.

1.6 Utilizando o gerador de relatórios

O Serviço de Geração de Relatórios fornece relatórios de aderência e status para o empreendimento. Os dados disponíveis são fornecidos para diretórios e grupos de usuários de um diretório. Os relatórios da Novell® fornecem feedback sobre os efeitos que os componentes individuais da política têm sobre os pontos de extremidade do empreendimento. As solicitações para esses relatórios são definidas na Política de Segurança (consulte Seção 2.2.4, "Gerador de Relatórios de Compatibilidade" na página 102) e podem fornecer dados úteis para a determinação de atualizações de política.

Selecione *Gerador de Relatórios* na barra de tarefas de *Auditoria de Ponto de Extremidade* ou no menu *Ver*. A lista de relatórios disponíveis será mostrada (clique nos ícones com sinal de adição ao lado de cada tipo de relatório para expandir a lista).

Para configurar relatórios, identifique a faixa de datas e outros parâmetros, como usuário ou localização. Para definir as datas, expanda a tela de calendário e selecione o mês e o dia. Clique no dia para mudar o parâmetro de data.

Clique em *Ver* para gerar o relatório.

Após a geração do relatório, você pode usar a barra de ferramentas para ver o relatório por meio do Console de Gerenciamento, para imprimir o relatório e para enviar por e-mail ou exportar o relatório como arquivo `.pdf`.

Ao analisar relatórios, use os botões de seta para navegar pelas páginas. Geralmente, os relatórios contêm gráficos na primeira página; os dados reunidos ficam nas páginas restantes, ordenados por data e tipo.

O botão *Impressora* permite que você imprima o relatório completo usando a impressora padrão do computador.

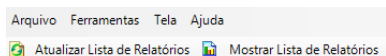
O botão *Exportar* grava o relatório como um arquivo PDF, uma planilha do Excel*, um documento do Word ou um arquivo RTF.

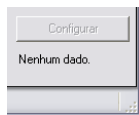
O botão *Árvore de Grupo* alterna uma lista de parâmetros para o lado do relatório. Selecione um desses parâmetros para detalhar mais o relatório. Clique no botão *Árvore de Grupo* para fechar a barra lateral.

O botão *Lupa* fornece um menu suspenso que permite ajustar o tamanho da tela atual.

O botão *Binóculos* abre uma janela de pesquisa.

Quando você passa o cursor do mouse sobre um determinado parâmetro, como nome de usuário ou nome de dispositivo, ele se transforma em uma lupa. Clique duas vezes sobre esse item específico para exibir um novo relatório sobre o objeto. Clique no botão *Fechar* para fechar a tela atual e retornar ao relatório original.

Para retornar à lista de relatórios, clique no ícone *Lista de Relatórios* acima da janela de relatórios.

Os relatórios só estarão disponíveis quando for feito o upload dos dados do ZENworks® Security Clients. Por padrão, o Serviço de Geração de Relatórios do ZENworks Endpoint Security Management é sincronizado a cada 12 horas. Isso significa que os dados originais de relatórios e alertas só estarão prontos 12 horas após a instalação do ZENworks Endpoint Security Manager. Para ajustar esse período, abra a ferramenta Configuração (consulte “Programação” na página 15) e ajuste o tempo de *Gerador de Relatórios do Cliente* de acordo com o número de minutos adequado às suas necessidades e ao seu ambiente.

Os botões *Configurar* e *Visualização* dos relatórios que não possuírem dados disponíveis ficarão cinza, com as palavras "Nenhum dado" escritas embaixo.

Os seguintes relatórios estão disponíveis:

- Seção 1.6.1, “Relatórios de Aderência” na página 30
- Seção 1.6.2, “Relatórios de Detalhamento de Alertas” na página 31

1.6.1 Relatórios de Aderência

Os Relatórios de Aderência fornecem informações de conformidade sobre a distribuição de políticas de segurança para usuários gerenciados. A pontuação de 100% de aderência indica que todos os usuários gerenciados registraram a entrada e receberam a política atual.

Os seguintes relatórios estão disponíveis:

* **Aderência de Registro de Entrada de Ponto de Extremidade:** Fornece um resumo dos dias decorridos desde o registro de entrada por ponto de extremidade do empreendimento e a duração da política atual. A média desses números é calculada para resumir o relatório. Esse relatório não requer variáveis. O relatório exibe os usuários por nome, pelas políticas designadas a eles, pelos dias desde o último registro de entrada e pela duração da política.
* **Versões de Cliente de Ponto de Extremidade:** Mostra a versão reportada mais recente do cliente em cada ponto de extremidade. Defina os parâmetros de data para gerar esse relatório.
* **Pontos de Extremidade que Nunca Registraram Entrada:** Lista as contas de usuários que se registraram no Serviço de Gerenciamento mas nunca registraram entrada no Serviço de Distribuição de uma atualização de política. Selecione um ou mais grupos para gerar o relatório.

  Esses usuários podem ser usuários do Console de Gerenciamento sem um Security Client instalado em seu nome.
* **Não-conformidade com Política de Grupo:** Mostra grupos em que alguns usuários não possuem a política correta. Um ou mais grupos podem gerar o relatório.
* **Histórico de Estado de Ponto de Extremidade por Máquina:** Exibe o status mais recente (em uma determinada faixa de datas) de pontos de extremidade protegidos pelo ZENworks Endpoint Security Management, agrupados por nome de máquina. Exibe o nome de usuário registrado, a política atual, a versão do cliente do ZENworks Endpoint Security Management e

o local de rede. Esse relatório requer uma faixa de datas. O administrador pode fazer o detalhamento clicando duas vezes em qualquer entrada para ver uma lista completa de relatórios de status de uma máquina específica.

- **Designação de Política:** Mostra quais usuários e grupos (contas) receberam a política especificada. Selecione a política desejada na lista e clique em *Ver* para executar o relatório.
- **Histórico de Estado de Ponto de Extremidade por Usuário:** Exibe o status mais recente (em uma determinada faixa de datas) de pontos de extremidade protegidos pelo ZENworks Endpoint Security Management, agrupados por nome de usuário. Exibe o nome de máquina, a política atual, a versão do cliente do ZENworks Endpoint Security Management e o local de rede. Esse relatório requer uma faixa de datas. O administrador pode fazer o detalhamento clicando duas vezes em qualquer entrada para ver uma lista completa de relatórios de status de um usuário específico.

1.6.2 Relatórios de Detalhamento de Alertas

Os Relatórios de Detalhamento de Alertas fornecem informações adicionais sobre alertas. Esses relatórios só exibem dados quando um alerta é acionado. Se você limpar um alerta, o relatório de alerta também será limpo. No entanto, os dados ainda estarão disponíveis em um relatório padrão.

Os seguintes relatórios estão disponíveis:

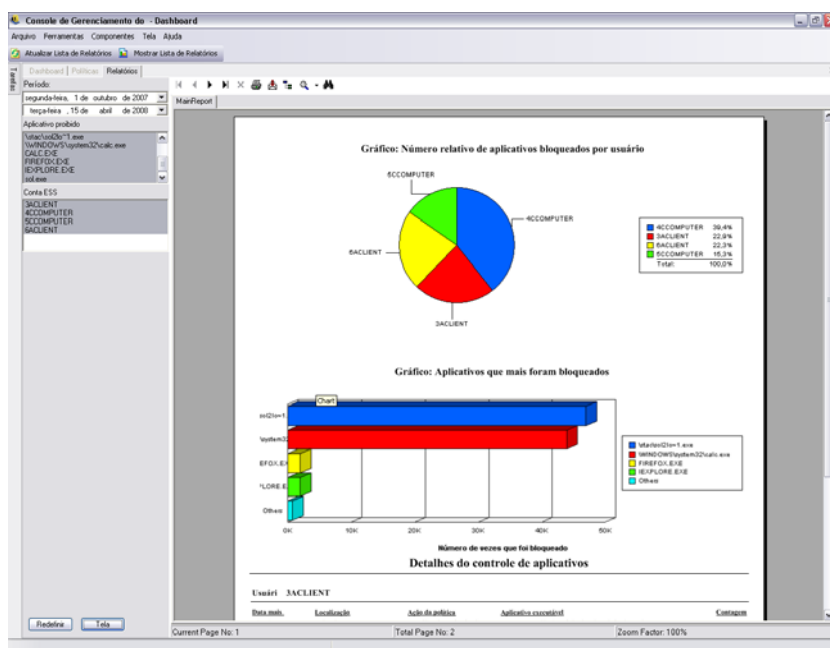
- **Dados de Alerta de Falsificação do Client:** Exibe instâncias em que um usuário fez uma tentativa não autorizada de modificar ou desabilitar o ZENworks Security Client.
- **Dados de Alerta de Arquivos Copiados:** Mostra as contas que copiaram dados para dispositivos de armazenamento removíveis.
- **Dados de Alerta de Versão Incorreta do Client:** Mostra o histórico do status do processo de Atualização do ZENworks Security Client.
- **Dados de Alerta de Política Incorreta do Client:** Mostra os usuários que não possuem a política correta.
- **Dados de Alerta de Falhas de Integridade:** Reporta o histórico de êxitos e falhas nas verificações de integridade do cliente.
- **Dados de Alerta de Tentativas de Anulação:** Mostra instâncias em que os mecanismos de autodefesa do cliente foram administrativamente anulados, concedendo controle privilegiado sobre o ZENworks Security Client.
- **Dados de Alerta de Exploração de Porta:** Mostra o número de pacotes bloqueados no número de diferentes portas (um grande número de portas pode indicar que ocorreu uma exploração de portas).
- **Dados de Alerta de Tentativa de Desinstalação:** Lista usuários que tentaram desinstalar o ZENworks Security Client.
- **Dados de Alerta de Ponto de Acesso Não Seguro:** Lista pontos de acesso não seguros detectados pelo ZENworks Security Client.
- **Dados de Alerta de Conexão com Ponto de Acesso Não Seguro:** Lista pontos de acesso não seguros conectados pelo ZENworks Security Client.

1.6.3 Relatórios de Controles de Aplicativo

Os Relatórios de Controles de Aplicativo exibem todas as tentativas não autorizadas feitas por aplicativos bloqueados para acessar a rede ou para executar sem permissão da política.

O seguinte relatório está disponível:

- **Detalhes do Controle de Aplicativo:** Exibe a data, a localização, a ação executada pelo ZENworks® Security Client, o aplicativo que tentou ser executado e o número de vezes que o aplicativo foi iniciado. As datas são exibidas em UTC.

Especifique os parâmetros de data, selecione os nomes de aplicativo na lista, selecione as contas de usuário e clique em *Ver* para executar o relatório.

1.6.4 Relatórios de Soluções de Criptografia

Se a criptografia de ponto de extremidade estiver ativada, os Relatórios de Soluções de Criptografia exibirão a transferência de arquivos de e para as pastas criptografadas.

Os seguintes relatórios estão disponíveis:

- **Atividade de Criptografia de Arquivo:** Mostra arquivos nos quais foi aplicada criptografia.
- **Exceções de Criptografia:** Mostra erros do sub-sistema de criptografia (por exemplo, um arquivo protegido não pôde ser decodificado porque o usuário não tinha as chaves certas).
- **Volumes de Criptografia de Arquivo:** Mostra volumes (por exemplo, unidades removíveis ou partições do disco rígido) gerenciados pela Solução de Criptografia da Novell.

1.6.5 Relatórios de Atividade de Ponto de Extremidade

Os Relatórios de Atividade de Ponto de Extremidade fornecem feedback sobre componentes de política individuais e o efeito que eles têm sobre a operação do ponto de extremidade.

Os seguintes relatórios estão disponíveis:

- **Pacotes Bloqueados por Endereço IP:** Exibe pacotes bloqueados filtrados por IP de Destino. As datas são exibidas em UTC.

  Selecione o IP de destino na lista e defina os parâmetros de data. O relatório mostra as datas, as localizações, as portas afetadas e o nome dos pacotes bloqueados.
- **Pacotes Bloqueados por Usuário:** Exibe pacotes bloqueados filtrados por usuário. As datas são exibidas em UTC. Os dados fornecidos são basicamente iguais aos dados de Pacotes Bloqueados por IP de Destino; no entanto, são separados por usuário.
- **Estatísticas de Uso da Rede por Usuário:** Lista pacotes enviados, recebidos ou bloqueados, bem como erros de rede, filtrados por usuários. Esse relatório requer uma faixa de datas. As datas são exibidas em UTC.
- **Estatísticas de Uso da Rede por Tipo de Adaptador:** Lista pacotes enviados, recebidos ou bloqueados, bem como erros de rede, filtrados por tipo de adaptador. Esse relatório requer uma faixa de datas e a localização. As datas são exibidas em UTC.

1.6.6 Relatórios de Atualizações de Ponto de Extremidade

Os Relatórios de Atualizações de Ponto de Extremidade exibem o status do processo de atualização do ZENworks Security Client (consulte "Atualização do ZSC" na página 63). As datas são exibidas em UTC.

Os seguintes relatórios estão disponíveis:

- **Porcentagem Gráfica de Falhas de Atualização do Security Client:** Exibe em forma de gráfico a porcentagem de Atualizações do ZENworks Security Client que apresentaram falha (e não foram remediadas). Não são exigidos parâmetros para gerar esse relatório.
- **Histórico do Status de Atualização do Security Client:** Mostra o histórico do status do processo de Atualização do ZENworks Security Client. Selecione a faixa de datas e clique em *Ver* para executar o relatório. O relatório mostra quais usuários registraram entrada e receberam a atualização.
- **Tipos de Gráfico de Atualizações do Security Client com Falha:** Mostra as Atualizações do ZENworks Security Client que apresentaram falha e não foram remediadas. Selecione a faixa de datas e clique em Ver para executar o relatório. O relatório mostra quais usuários registraram entrada, mas tiveram uma falha na instalação da atualização.

1.6.7 Relatórios de Autodefesa do Client

Os Relatórios de Autodefesa do Client informam quando algum usuário tenta modificar ou desabilitar o ZENworks® Security Client.

O seguinte relatório está disponível:

- **Tentativas de Hack do ZENworks Security Client:** Reporta instâncias em que um usuário tentou modificar ou desabilitar o ZENworks Security Client sem autorização. Datas exibidas em UTC.

  Insira os parâmetros de data e clique em *Ver* para executar o relatório.

1.6.8 Relatórios de Aplicação de Integridade

Os Relatórios de Aplicação de Integridade reportam resultados de integridade antivírus/anti-spyware.

Os seguintes relatórios estão disponíveis:

- **Histórico de Integridade do Cliente:** Reporta êxitos ou falhas nas verificações de integridade do cliente. As datas são exibidas em UTC.

  Selecione a faixa de datas do relatório, das regras de integridade e dos nomes de usuário.
- **Falhas de Integridade Não Remediadas por Regra:** Reporta regras de integridade e testes que falharam e ainda não foram remediados.

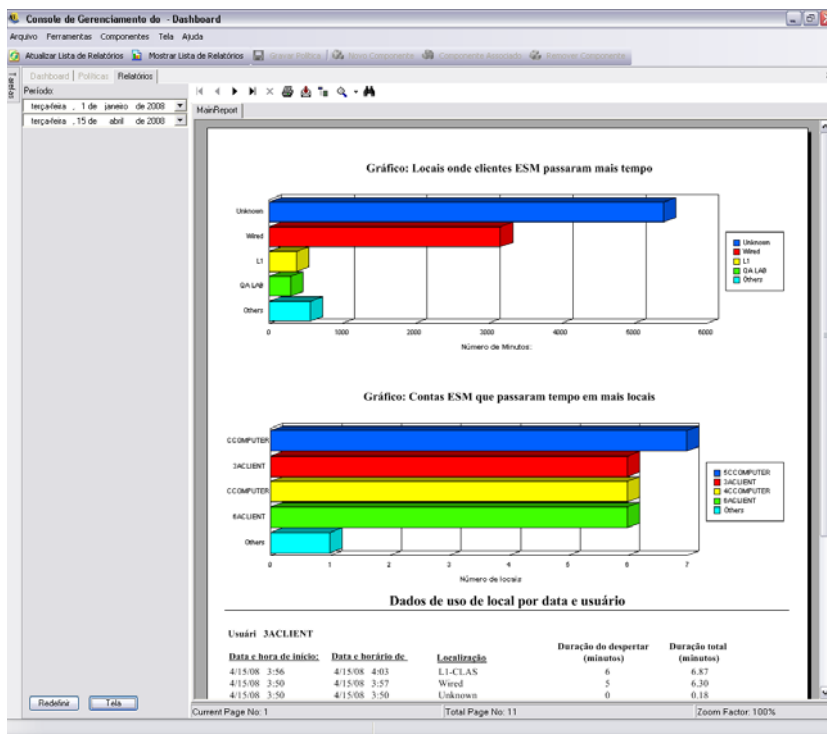
  Selecione as regras de integridade e clique em *Ver* para executar o relatório.
- **Falhas de Integridade Não Remediadas por Usuário:** Reporta usuários que foram reprovados nos testes de integridade e ainda não foram remediados.

  Selecione os nomes de usuário e clique em *Ver* para executar o relatório.

1.6.9 Relatórios de Localização

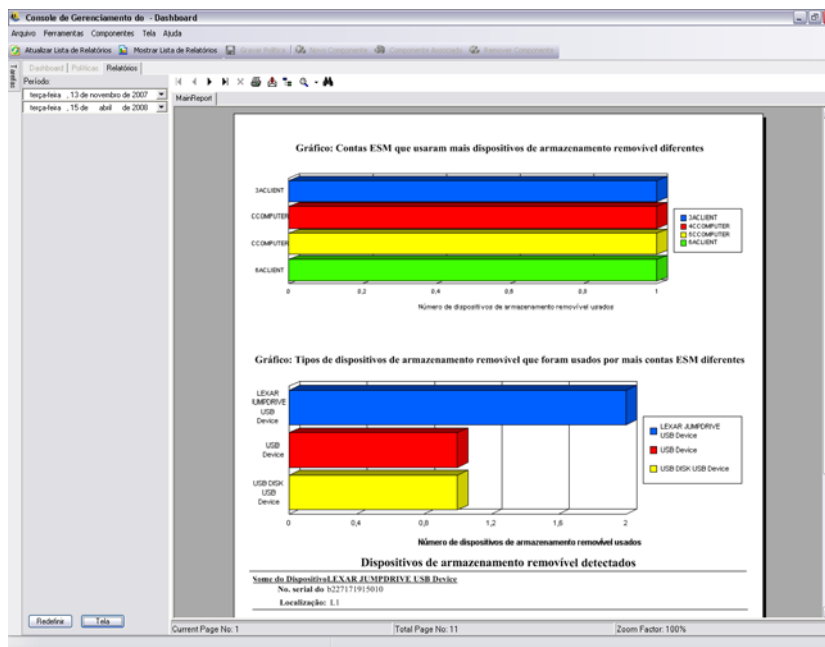
Os Relatórios de Localização fornecem dados sobre a utilização de localizações, como as localizações mais usadas pelos usuários.

O seguinte relatório está disponível:

Dados de Uso de Localização por Data e Usuário: Fornece informações coletadas em clientes individuais sobre quais localizações são usadas e quando. As datas são exibidas em UTC. As localizações exibidas são as localizações usadas pelo usuário; as localizações não usadas não são exibidas. Selecione uma faixa de datas para gerar o relatório.

1.6.10 Relatórios de Conformidade de Conteúdo de Saída

Os Relatórios de Conformidade de Conteúdo de Saída contêm informações sobre o uso de unidades removíveis e identifica quais arquivos foram carregados para essas unidades.

Os seguintes relatórios estão disponíveis:

- **Atividade de Armazenamento Removível por Conta:** Mostra as contas que copiaram dados para armazenamento removível. Não são exigidos parâmetros para gerar esse relatório.
- **Atividade de Armazenamento Removível por Dispositivo:** Mostra os dispositivos de armazenamento removíveis para os quais foram copiados arquivos. Selecione a faixa de datas, os nomes de usuário e as localizações para gerar o relatório.
- **Cópias de Armazenamento Removível por Conta:** Mostra arquivos que foram copiados de dispositivos de armazenamento removíveis para dispositivos gerenciados.
- **Dispositivos de Armazenamento Removível Detectados:** Mostra dispositivos de armazenamento removíveis que foram detectados no ponto de extremidade. Selecione a faixa de datas, os nomes de usuário e as localizações para gerar o relatório.

- **Gráfico 7 Dias de atividade de armazenamento removível por conta:** Exibe um gráfico contendo as contas que recentemente copiaram dados para armazenamento removível. Digite a faixa de datas para gerar esse relatório.

1.6.11 Relatório de anulação administrativa

O Relatório de Anulação Administrativa mostra as instâncias em que os mecanismo de autodefesa do cliente foram anulados administrativamente, concedendo controle privilegiado sobre o ZENworks® Security Client.

O seguinte relatório está disponível:

- **Anulações do ZENworks Security Client:** Mostra tentativas de anulação bem-sucedidas por usuário e data. As datas são exibidas em UTC.

  Selecione o usuário e a faixa de datas e clique em *Ver* para executar o relatório.

1.6.12 Relatórios de Atualizações de Ponto de Extremidade

Os Relatórios de Atualizações de Ponto de Extremidade exibem o status do processo de Atualização do ZENworks® Security Client (consulte "Atualização do ZSC" na página 63). As datas são exibidas em UTC.

Os seguintes relatórios estão disponíveis:

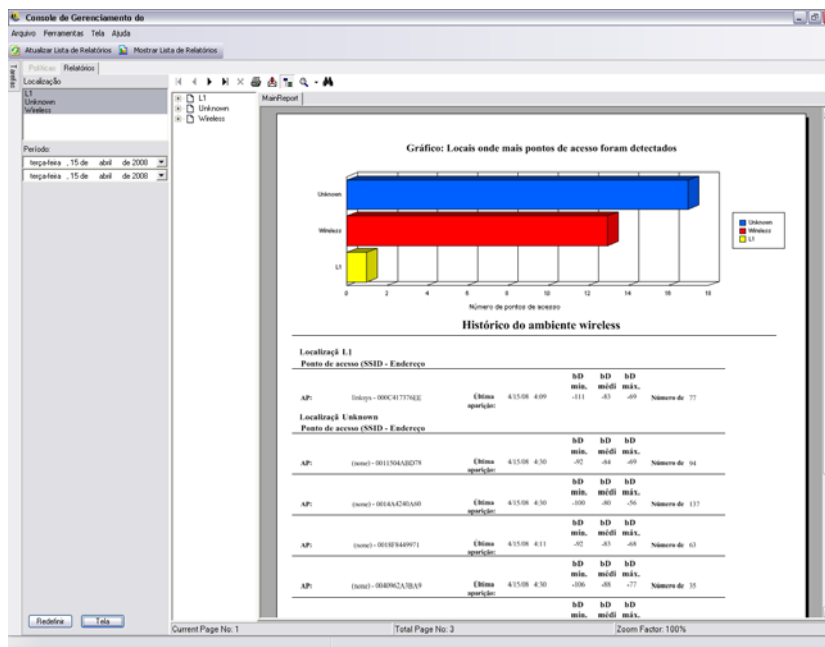
- **Porcentagem Gráfica de Falhas de Atualização do Security Client:** Exibe em forma de gráfico a porcentagem de Atualizações do ZENworks Security Client que apresentaram falha e não foram remediadas. Não são exigidos parâmetros para gerar esse relatório.

- **Histórico do Status de Atualização do Security Client:** Mostra o histórico do status do processo de Atualização do ZENworks Security Client. Selecione a faixa de datas e clique em *Ver* para executar o relatório. O relatório mostra quais usuários registraram entrada e receberam a atualização.
- **Tipos de Gráfico de Atualizações do Security Client com Falha:** Mostra as Atualizações do ZENworks Security Client que apresentaram falha e não foram remediadas. Selecione a faixa de datas e clique em *Ver* para executar o relatório. O relatório mostra quais usuários registraram entrada, mas tiveram uma falha na instalação da atualização.

1.6.13 Relatórios de Aplicação de Ambiente Sem Fio

Os Relatórios de Aplicação de Ambiente Sem Fio fornecem informações sobre os ambientes Wi-Fi aos quais o ponto de extremidade está exposto.

Os seguintes relatórios estão disponíveis:

- **Disponibilidade de Conexão Sem Fio:** Exibe os pontos de acesso disponíveis para conexão por política e localização. Inclui o canal, o SSID e o endereço MAC e informa se o ponto de acesso foi criptografado ou não.
- **Tentativas de Conexão Sem Fio:** Fornece uma lista de pontos de acesso aos quais os dispositivos tentam se conectar, por localização e conta.
- **Histórico de Ambiente Sem Fio:** Fornece uma pesquisa de todos os pontos de acesso detectados, independentemente da propriedade. Inclui a freqüência e a força do sinal e informa se o ponto de acesso foi criptografado ou não. As datas são exibidas em UTC. Selecione as localizações desejadas e a faixa de datas para gerar esse relatório.

1.7 Utilizando a Solução de Criptografia de Armazenamento do ZENworks

A Solução de Criptografia de Armazenamento do ZENworks® fornece um gerenciamento de segurança completo e centralizado de todos os dados móveis por meio da aplicação ativa de uma política de criptografia corporativa no próprio ponto de extremidade.

A Solução de Criptografia de Armazenamento do ZENworks permite:

- Criar de forma centralizada, distribuir, aplicar e auditar políticas de criptografia em todos os pontos de extremidade e dispositivos de armazenamento removíveis.
- Criptografar todos os arquivos gravados ou copiados em um diretório específico em todas as partições de disco fixas do disco rígido.
- Criptografar todos os arquivos copiados para dispositivos de armazenamento removíveis.
- Compartilhar arquivos livremente dentro de uma organização e, ao mesmo tempo, bloquear acesso não autorizado aos arquivos.
- Compartilhar arquivos protegidos por senha e criptografados com pessoas de fora da organização por meio de um utilitário de decodificação disponível.
- Atualizar, fazer backup e recuperar chaves usando políticas, sem perder dados.

1.7.1 Noções básicas sobre a Solução de Criptografia de Armazenamento do ZENworks

A criptografia de dados é aplicada por meio da criação e da distribuição de políticas de segurança de criptografia de dados. Os dados confidenciais do ponto de extremidade são armazenados em uma pasta criptografada. O usuário pode acessar e copiar esses dados fora da pasta criptografada, bem como compartilhar os arquivos; entretanto, enquanto estiverem nessa pasta, os dados permanecerão criptografados. Se qualquer pessoa que não seja um usuário autorizado da máquina tentar ler os dados, não conseguirá. Quando a política é ativada, uma pasta criptografada `Safe Harbor` é adicionada ao diretório raiz dos volumes que não são do sistema no ponto de extremidade.

Os dados confidenciais armazenados em uma chave USB ou em outro dispositivo de mídia removível serão imediatamente criptografados e só poderão ser lidos em máquinas do mesmo grupo de política. Uma pasta de compartilhamento pode ser ativada opcionalmente. Isso permitirá ao usuário compartilhar os arquivos com pessoas de fora de seu grupo de políticas usando uma senha (consulte “Criptografia de Dados” na página 61).

1.7.2 Compartilhando arquivos criptografados

Os usuários do mesmo grupo de política (os usuários que receberam a mesma política de segurança) terão as chaves para acessar os dados armazenados no ponto de extremidade, bem como os dados movidos para chaves USB e outros dispositivos removíveis.

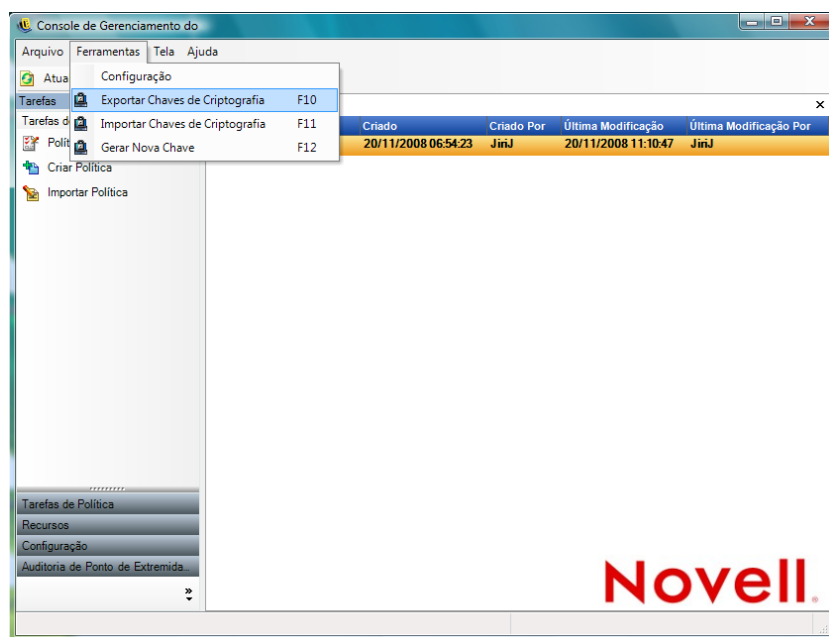
Os usuários de um grupo de política separado (com a criptografia ativada), poderão acessar os dados criptografados colocados na pasta `Arquivos Compartilhados` usando uma senha de acesso. Esses usuários não poderão ler os arquivos criptografados que estiverem fora da pasta `Arquivos Compartilhados`.

Os usuários cujas políticas não estiverem criptografadas e os usuários que não tiverem o ZENworks Security Client no computador (por exemplo, prestadores de serviço externos) não poderão ler os arquivos fora da pasta `Arquivos Compartilhados`. É preciso ter o Utilitário de Decodificação de Arquivos do ZENworks® para ler os arquivos com acesso à rede. Para obter mais informações, consulte Seção 1.9, "Utilizando o Utilitário de Decodificação de Arquivos do ZENworks" na página 40.

1.8 Utilizando o gerenciamento de chaves

O gerenciamento de chaves permite fazer o backup, importar e atualizar uma chave criptográfica. É recomendável que você exporte e grave as chaves criptográficas para assegurar que os dados possam ser decodificados no caso de uma falha de sistema ou de uma mudança repentina de política.

A chave comum é a chave criptográfica padrão usada para todos os agentes de criptografia de dados. A chave criptográfica poderá ser atualizada se estiver comprometida, ou como precaução de segurança. A geração de uma nova chave comum resulta em uma diminuição temporária de desempenho, enquanto o conteúdo gerenciado é criptografado novamente.

Para acessar os controles de chave criptográfica, vá para o menu *Ferramentas* do Console de Gerenciamento.

1.8.1 Exportando chaves criptográficas

Para fins de backup e para enviar a chave a outra instância do Serviço de Gerenciamento, exporte o conjunto de chaves criptográficas atual para uma localização de arquivo indicada.

1. Clique em *Ferramentas > Exportar Chaves Criptográficas*.
2. Especifique o caminho com um nome de arquivo ou clique no botão *Procurar* para procurar e selecionar uma localização de arquivo.
3. Especifique uma senha. A chave não pode ser importada sem essa senha.
4. Clique em *OK*.

Todos os arquivos de chaves do banco de dados são incluídos no arquivo exportado.

1.8.2 Importando chaves criptográficas

É possível importar chaves de um backup ou de outra instância do Serviço de Gerenciamento. Isso permite que os pontos de extremidade gerenciados por esse Serviço de Gerenciamento leiam arquivos protegidos por outras instalações do ZENworks Endpoint Security Management. Quando você importa chaves, as duplicatas são ignoradas. As chaves importadas tornam-se parte do conjunto de chaves e não substituem a chave comum atual. Todas as chaves são passadas para baixo quando uma nova política é publicada.

1. Clique em *Ferramentas* > *Importar Chaves Criptográficas*.
2. Especifique o nome do arquivo, incluindo a localização do arquivo, ou clique no botão *Procurar* para procurar e selecionar o arquivo de chave.
3. Especifique a senha da chave criptográfica.
4. Clique em *OK* para importar a chave para o banco de dados.

1.8.3 Gerando uma nova chave

1. Clique em *Ferramentas* > *Gerar Nova Chave*.

Todas as chaves anteriores estão armazenadas na política.

1.9 Utilizando o Utilitário de Decodificação de Arquivos do ZENworks

O Utilitário de Decodificação de Arquivos do ZENworks® extrai dados protegidos da pasta `Arquivos Compartilhados` em dispositivos de armazenamento removíveis criptografados. Essa ferramenta simples pode ser fornecida a terceiros para que eles possam acessar arquivos da pasta `Arquivos Compartilhados`. No entanto, a ferramenta não pode ser colocada no dispositivo de armazenamento removível.

- Seção 1.9.1, “Usando o Utilitário de Decodificação de Arquivos” na página 40
- Seção 1.9.2, “Configurando o Utilitário de Decodificação de Arquivos” na página 41

As seções a seguir contêm mais informações:

1.9.1 Usando o Utilitário de Decodificação de Arquivos

Para usar o Utilitário de Decodificação de Arquivos:

1. Conecte o dispositivo de armazenamento à porta apropriada do computador.
2. Abra o Utilitário de Decodificação de Arquivos.
3. Procure o diretório `Arquivos Compartilhados` do dispositivo de armazenamento e selecione o arquivo desejado.
4. Para extrair diretórios (pastas) em vez de arquivos, clique no botão *Avançado* e selecione *Diretórios*, em seguida procure o diretório apropriado (clique em *Básico* para retornar à tela padrão).

5. Procure e selecione o destino na máquina local onde esses arquivos serão armazenados.
6. Clique em *Extrair*.

Para monitorar a transação, clique no botão *Mostrar Progresso*.

1.9.2 Configurando o Utilitário de Decodificação de Arquivos

O Utilitário de Decodificação de Arquivos pode ser configurado no modo de administrador com o conjunto de chaves atual e pode extrair todos os dados de um dispositivo de armazenamento criptografado. Não é recomendável usar essa configuração porque ela pode comprometer todas as chaves atuais usadas pela Solução de Criptografia de Armazenamento do ZENworks; no entanto, em casos em que não haja outro modo de recuperar os dados, essa configuração pode ser necessária.

Para configurar a ferramenta:

1. Crie um atalho para o Utilitário de Decodificação de Arquivos dentro do diretório atual.
2. Clique o botão direito do mouse no atalho e, em seguida, clique em *Propriedades*.
3. No final do nome de destino, depois das aspas, digite -k (por exemplo: `"C:\Admin Tools\stdecrypt.exe" -k`).
4. Clique em *Aplicar* > *OK*.
5. Abra a ferramenta usando o atalho e clique em *Avançado*.
6. Clique no botão *Carregar Chaves* para abrir a caixa de diálogo Importar Chave.
7. Procure o arquivo de chaves e especifique a senha das chaves.

Agora, todos os arquivos criptografados com essas chaves podem ser extraídos.

1.10 Utilizando o Override-Password Key Generator

Interrupções de produtividade ocorridas devido a restrições de conectividade, execução de software desabilitado ou acesso a dispositivos de armazenamento removíveis provavelmente são causadas pela política de segurança aplicada pelo ZENworks® Security Client. Em geral, a mudança de localizações ou de configurações do firewall derruba essas restrições e restaura a funcionalidade interrompida. No entanto, em alguns casos, a restrição pode ser implementada de forma que os usuários tenham restrições em todas as localizações e configurações do firewall, ou que não consigam fazer uma mudança de localização ou de configuração do firewall.

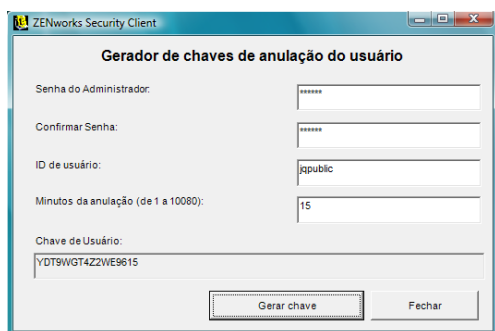
Quando isso ocorre, as restrições na política atual podem ser eliminadas com uma anulação de senha que permita o uso até que a política seja modificada. Esse recurso permite que o administrador configure a anulação de proteção por senha para usuários e funcionalidades específicos, o que permite temporariamente a realização das atividades necessárias.

As anulações de senha desabilitam a política de segurança atual e restauram a política padrão Todos Abertos por um período predefinido. Após a expiração do limite de tempo, a política atual ou atualizada é restaurada. A senha de uma política é definida nas configurações de Regras Globais da política de segurança.

A substituição de senha faz o seguinte:

- Anula o bloqueio de aplicativos

* Permite que os usuários mudem localizações
* Permite que os usuários mudem configurações do firewall
* Anula o controle de hardware (unidades USB, CD-ROM, etc.)

A senha digitada na política nunca deve ser emitida para um usuário. Use o Override-Password Key Generator para gerar uma chave válida por um curto período.

Para gerar uma chave de anulação:

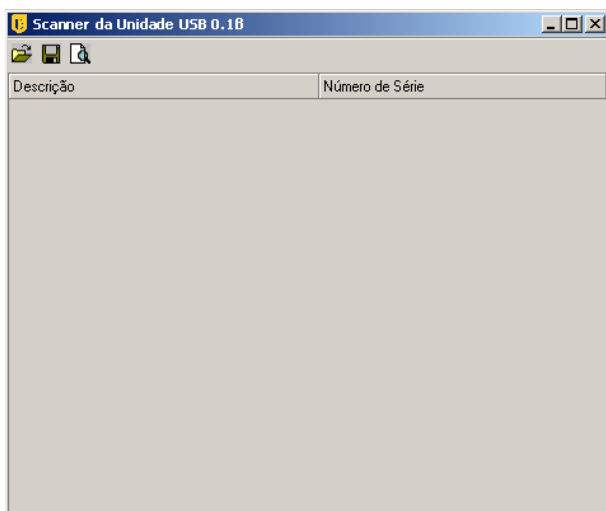
1. Abra o Override-Password Key Generator (*Iniciar* > *Todos os Programas* > *Novell* > *Console de Gerenciamento do ESM* > *Override-Password Generator*).
2. Especifique a senha da política no campo *Senha do Administrador* e confirme-a no campo seguinte.
3. Especifique o nome de usuário com o qual o usuário final efetuou login.
4. Especifique em quanto tempo a política deverá ser desabilitada.
5. Clique no botão *Gerar Chave* para gerar uma chave de anulação.

Essa chave pode ser lida para o usuário durante uma chamada para o suporte técnico ou pode ser copiada e colada em um e-mail. Em seguida, o usuário digita a chave na janela Administração do ZENworks Security Client (consulte o *Guia do Usuário do Security Client do ZENworks Endpoint Security Management*). Essa chave é válida para a política desse usuário e apenas durante o tempo especificado. Depois que a chave for usada, ela não poderá ser usada novamente.

Observa o: Se o usuário efetuar logoff ou reinicializar a máquina durante a anulação de senha, a senha irá expirar e uma nova senha precisará ser emitida.

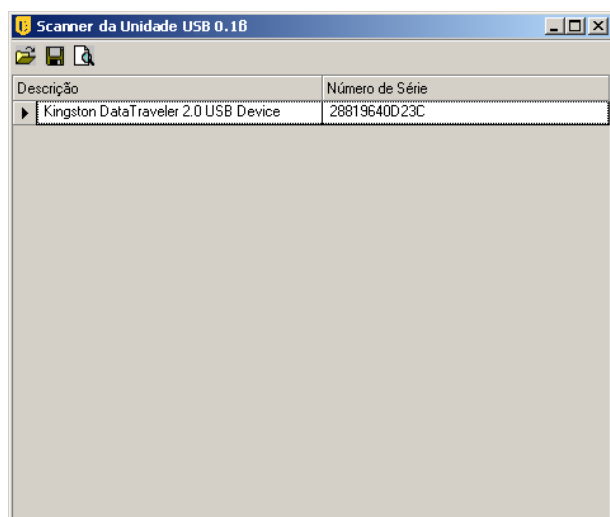
Se uma nova política for escrita antes da expiração do limite de tempo, o usuário deverá ser instruído a verificar se há uma atualização de política, em vez de clicar no botão *Carregar Política* na caixa de diálogo Sobre do ZENworks Security Client.

1.11 Scanner da Unidade USB

Para gerar e importar para uma política uma lista de dispositivos USB autorizados, use a ferramenta opcional Scanner da Unidade USB (incluída no pacote de instalação).

Para gerar uma lista de dispositivos autorizados:

1. Abra o aplicativo Scanner da Unidade USB.

   Observa o: Esta é uma instalação separada do Serviço de Gerenciamento e do Console de Gerenciamento. Um atalho para a ferramenta é exibido na área de trabalho.

2. Insira um dispositivo USB na porta USB do computador. O dispositivo precisa ter um número de série.
3. Clique no ícone *Explorar* ( ). O nome e o número de série do dispositivo são exibidos nos campos apropriados.

4. Repita a Etapa 2 e a Etapa 3 até que todos os dispositivos tenham sido inseridos na lista.
5. Clique no ícone `Gravar` ( ).

Consulte Seção , "Dispositivos Preferidos" na página 54 para obter instruções sobre como importar a lista para uma política.

Para editar um arquivo gravado, clique no ícone *Procurar* ( ) e abra o arquivo.

Criando e distribuindo políticas de segurança

2

O ZENworks® Security Client usa políticas de segurança para aplicar segurança de localização a usuários móveis. As decisões sobre disponibilidade de portas de rede, disponibilidade de aplicativos de rede, acesso a dispositivos de armazenamento de arquivos e conectividade por fio ou Wi-Fi são determinadas pelo administrador para cada local.

As políticas de segurança podem ser criadas personalizadas para a empresa, para grupos de usuários individuais ou para usuários/máquinas individuais. As políticas de segurança podem conceder produtividade completa aos funcionários, ao mesmo tempo em que protegem o ponto de extremidade, ou podem permitir que o usuário execute apenas determinados aplicativos e tenha somente hardwares autorizados disponíveis para ele.

As seções a seguir contêm mais informações:

2.1 Navegando no Console de Gerenciamento

Para começar a criar uma política de segurança:

1. No Console de Gerenciamento, clique em *Arquivo* > *Criar Nova Política*.
2. Especifique o nome da nova política e clique em *Criar* para exibir o Console de Gerenciamento com a barra de ferramentas e as guias da política.

As seções a seguir descrevem a interface do usuário do Console de Gerenciamento no que se refere à criação e à distribuição de políticas de segurança por meio do ZENworks® Endpoint Security Management:

2.1.1 Utilizando as guias e a árvore da política

Para escrever ou editar uma política de segurança, navegue pelas guias disponíveis na parte superior do Console de Gerenciamento e use as opções da árvore *Configurações Globais* no painel esquerdo.

Estas são algumas das guias disponíveis:

- **Configurações de Política Global:** As Configurações de Política Global são aplicadas como padrão em toda a política; não são específicas de local.

  As Configurações de Política Global permitem definir as seguintes configurações:

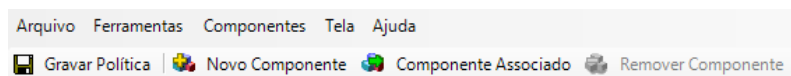
  - Configurações de Política
  - Controle Sem Fio

- Hardware de Comunicação
- Controle de Dispositivo de Armazenamento
- Conectividade USB
- Criptografia de Dados
- ZENworks Security Client
- Imposição de VPN

- **Localizações:** Essas regras de política são aplicadas a um determinado tipo de local, quer esse local seja especificado como uma única rede ou como um tipo de rede (por exemplo, um restaurante ou um aeroporto).
- **Regras de Integridade e Correção:** Essas regras garantem que softwares essenciais (como antivírus e spyware) estejam em execução e atualizados no dispositivo.
- **Gerador de Relatórios de Compatibilidade:** Informa a política se os dados de geração de relatórios (inclusive os tipos de dados) são coletados para esse política específica.
- **Publicar:** Publica a política concluída para usuários individuais, grupos de usuários do serviço de diretório e máquinas individuais.

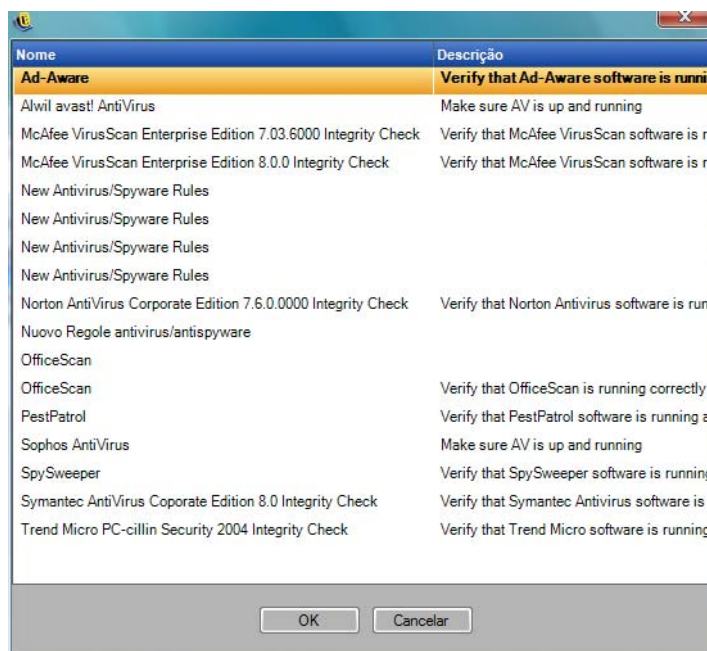
A árvore da política exibe componentes de subconjunto disponíveis para as categorias com guias. Por exemplo, a guia *Configurações de Política Global* inclui subconjuntos de *Configurações de Política*, *Controle Sem Fio*, *Hardware de Comunicação* e *Controle de Dispositivo de Armazenamento*. Apenas os itens contidos na página principal de subconjuntos são exigidos para a definição de uma categoria. Os subconjuntos restantes são componentes opcionais.

2.1.2 Utilizando a barra de ferramentas da política

A barra de ferramentas da política contém seis controles. O controle *Gravar Política* está disponível por toda a criação da política, mas os controles de componentes só estão disponíveis nas guias *Localizações* e *Remediação e Integridade*.

Explicações sobre as ferramentas são fornecidas a seguir:

- **Gravar Política:** Grava a política em seu estado atual.

> **Importante:** À medida que você completa cada subconjunto de componentes, é altamente recomendável clicar no ícone *Gravar* da barra de ferramentas *Política*. Se forem inseridos dados incompletos ou incorretos em um componente, a tela de notificação de erros será exibida (consulte Seção 2.2.6, “Notificação de erros” na página 106 para obter mais detalhes).

- **Novo Componente:** Cria um novo componente em um subconjunto de Localização ou Integridade. Depois que a política é gravada, um novo componente fica disponível para associação em outras políticas.
- **Associar Componente:** Abra a tela Selecionar Componente do subconjunto atual. Os componentes disponíveis englobam todos os componentes predefinidos incluídos na instalação e todos os componentes criados em outras políticas.

Importante: As mudanças feitas em componentes associados afetam todas as outras instâncias do componente.

Por exemplo, você pode criar um único componente de Localização chamado Trabalho que defina as configurações de segurança e de ambiente da rede corporativa a serem aplicadas sempre que um ponto de extremidade entrar nesse ambiente. Em seguida, esse componente poderá ser aplicado a todas as políticas de segurança. As atualizações nas configurações de ambiente ou de segurança só precisam ser feitas no componente de uma política. Em seguida, o mesmo componente será atualizado em todas as outras políticas às quais ele está associado.

Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

- **Remover Componente:** Remove um componente da política. O componente ainda está disponível para associação nesta e em outras políticas.
- **Atualizar Lista de Políticas:** Atualiza a lista de políticas.
- **Lista de Relatórios:** Exibe a lista de relatórios.

2.2 Criando políticas de segurança

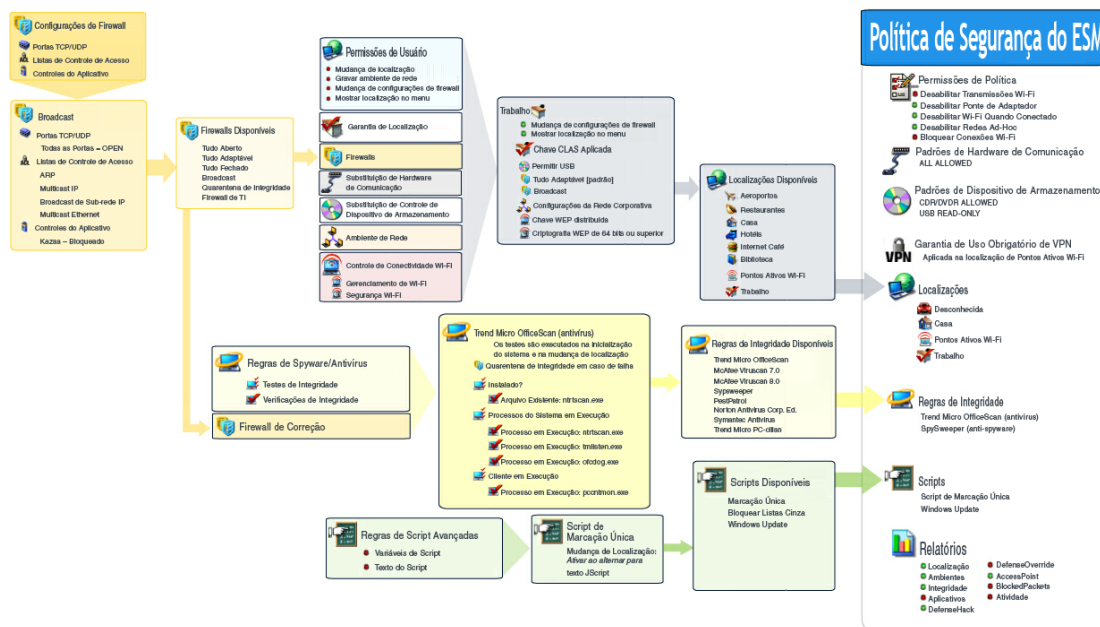
1. No Console de Gerenciamento, clique em *Arquivo > Criar Nova Política*.
2. Especifique o nome da nova política e clique em *Criar* para exibir o Console de Gerenciamento com a barra de ferramentas e as guias da política.
3. Para definir as configurações de política, use as informações contidas nas seguintes seções:

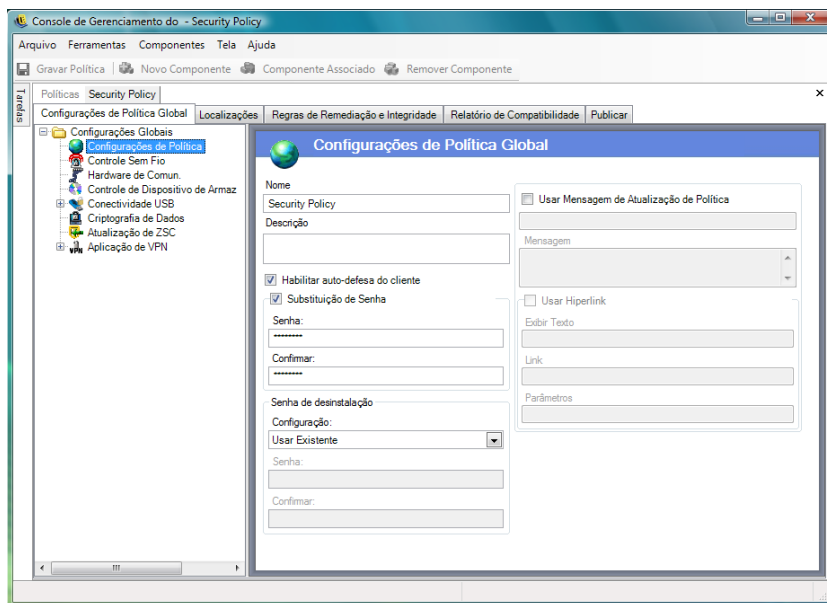
- Seção 2.2.1, “Configurações de Política Global” na página 48
- Seção 2.2.2, “Localizações” na página 69
- Seção 2.2.3, “Regras de Integridade e Correção” na página 94
- Seção 2.2.4, “Gerador de Relatórios de Compatibilidade” na página 102
- Seção 2.2.5, “Publicar” na página 104

- Seção 2.2.6, “Notificação de erros” na página 106
- Seção 2.2.7, “Mostrar Uso” na página 106

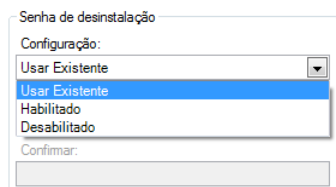
Para criar políticas de segurança, defina todas as configurações globais (comportamentos padrão); em seguida, crie e associe os componentes existentes da política, como localizações, firewalls e regras de integridade; por fim, estabeleça o gerador de relatórios de conformidade da política.

Os componentes são criados em uma política fictícia ou são associados de outras políticas. Para suas primeiras políticas, você deve criar todos os locais exclusivos, configurações de firewall e regras de integridade da empresa. Esses componentes são armazenados no banco de dados do Serviço de Gerenciamento para possível uso futuro em outras políticas.

O diagrama abaixo mostra os componentes de cada nível e uma política resultante das seleções.

2.2.1 Configurações de Política Global

As configurações globais da política são aplicadas como padrões básicos da política. Para acessar esse controle, vá para o Console de Gerenciamento e clique na guia *Configurações de Política Global*.

As seções a seguir contêm mais informações sobre as configurações que você pode definir em âmbito global:

- "Configurações de Política" na página 49
- "Controle Sem Fio" na página 50
- "Hardware de Comunicação" na página 51
- "Controle de Dispositivo de Armazenamento" na página 52
- "Conectividade USB" na página 55
- "Criptografia de Dados" na página 61
- "Atualização do ZSC" na página 63
- "Aplicação de VPN" na página 64
- "Mensagens Personalizadas para o Usuário" na página 67
- "Hiperlinks" na página 68

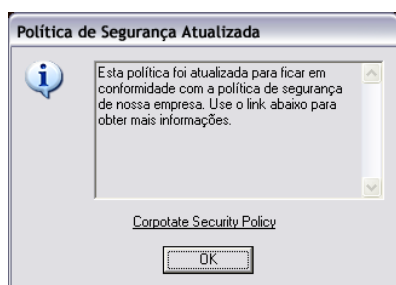
Configurações de Política

As principais configurações globais incluem:

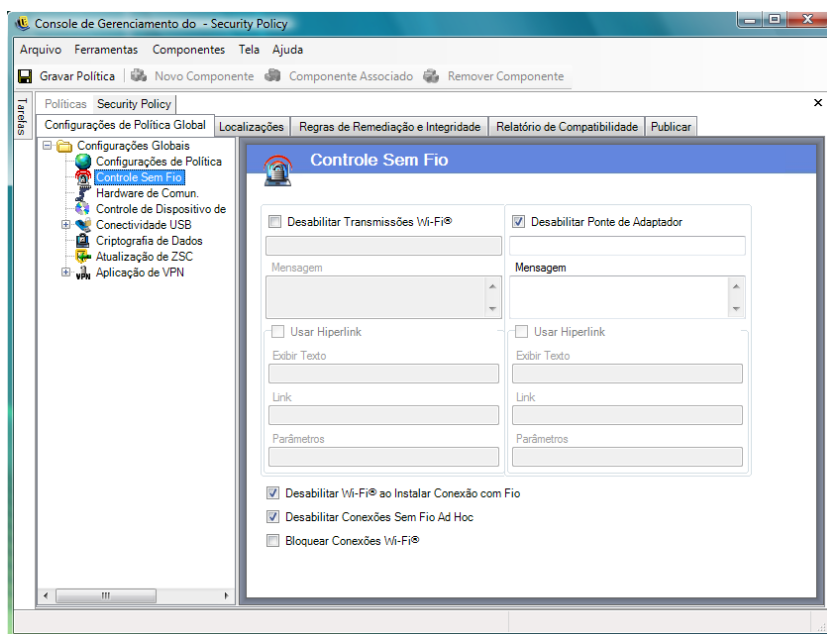
- **Nome e Descrição:** O nome da política é especificado no começo do processo de criação. Você pode editar o nome ou fornecer uma descrição da política.
- **Habilitar autodefesa do cliente:** A autodefesa do cliente pode ser habilitada ou desabilitada por política. Se você mantiver essa caixa marcada, a autodefesa do cliente ficará ativa. Se você desmarcar a caixa, a autodefesa do cliente será desativada em todos os pontos de extremidade que usarem essa política.
- **Anulação de Senha:** Esse recurso permite que um administrador defina uma anulação de senha que pode desabilitar temporariamente a política por um período específico. Marque a caixa *Anulação de Senha* e especifique a senha no campo fornecido. Insira a senha novamente

no campo de confirmação. Use essa senha no Override Password Generator para gerar a chave de senha para essa política. Para obter mais informações, consulte Seção 1.10, “Utilizando o Override-Password Key Generator” na página 41.

Aviso: É altamente recomendável que essa senha não seja fornecida aos usuários. Use o Override Password Generator para gerar uma chave temporária para eles.

- **Senha de Desinstalação:** É recomendável que cada ZENworks* Security Client seja instalado com uma senha de desinstalação para impedir que os usuário desinstalem o software. Normalmente, essa senha é configurada na instalação; no entanto, ela pode ser atualizada, habilitada ou desabilitada por meio da política.

  Selecione uma das seguintes configurações na lista suspensa:
  - **Usar Existente:** Essa é a configuração padrão. Mantém a senha atual inalterada.
  - **Habilitado:** Ativa ou muda uma senha de desinstalação. Especifique a nova senha e depois confirme-a.
  - **Desabilitado:** Desativa o requisito de senha de desinstalação.
- **Usar Mensagem de Atualização de Política:** Você poderá exibir uma mensagem personalizada para o usuário sempre que a política for atualizada. Clique na caixa de seleção e especifique as informações da mensagem nos campos fornecidos.
- **Usar Hiperlink:** Você pode incluir um hiperlink em informações adicionais, políticas corporativas, etc (para obter mais informações, consulte “Hiperlinks” na página 68).

Controle Sem Fio

O Controle Sem Fio define globalmente os parâmetros de conectividade do adaptador para proteger o ponto de extremidade e a rede. Para acessar esse controle, clique na guia *Configurações de Política Global* e, em seguida, clique no ícone *Controle Sem Fio* na árvore de política à esquerda.

As configurações de controle sem fio incluem o seguinte:

- **Desabilitar Transmissões Wi-Fi:** Desabilita globalmente todos os adaptadores Wi-Fi, o que inclui o silenciamento completo de um rádio Wi-Fi interno.

  Você pode optar por exibir uma mensagem personalizada para o usuário e um hiperlink quando o usuário tentar ativar uma conexão Wi-Fi. Consulte "Mensagens Personalizadas para o Usuário" na página 67 para obter mais informações.
- **Desabilitar Ponte de Adaptador:** Desabilita globalmente a funcionalidade de ponte de rede incluída no Windows* XP, que permite que o usuário interligue vários adaptadores e atue como um hub na rede.

  Você pode optar por exibir uma mensagem personalizada para o usuário e um hiperlink quando o usuário tentar ativar uma conexão Wi-Fi. Consulte "Mensagens Personalizadas para o Usuário" na página 67 para obter mais informações.
- **Desabilitar Wi-Fi Quando Conectado:** Desabilita globalmente todos os adaptadores Wi-Fi quando o usuário usa uma conexão com fio (LAN pela NIC).
- **Desabilitar Redes AdHoc:** Desabilita globalmente toda conectividade ad hoc, o que faz com que a conectividade Wi-Fi seja aplicada em uma rede (por exemplo, por um ponto de acesso) e restringe todas as redes não-hierárquicas desse tipo.
- **Bloquear Conexões Wi-Fi:** Bloqueia globalmente as conexões Wi-Fi sem silenciar o rádio Wi-Fi. Use essa configuração quando desejar desabilitar conexões Wi-Fi, mas quiser usar pontos de acesso para a detecção de local. Consulte Seção 2.2.2, "Localizações" na página 69 para obter mais informações.

Hardware de Comunicação

As configurações de hardwares de comunicação controlam, por localização, que tipos de hardware podem se conectar nesse ambiente de rede.

Observa o: Você pode definir os controles de hardware de comunicação globalmente na guia *Configurações de Política Global* ou pode defini-los para localizações individuais na guia *Localizações*.

Para definir os controles de hardware de comunicação globalmente, clique na guia *Configurações de Política Global*, expanda *Configurações Globais* na árvore e clique em *Hardware de Comunicação*.

Para definir os controles de hardware de comunicação para uma localização específica, clique na guia *Localizações*, expanda a localização desejada na árvore e clique em *Hardware de Comunicação*. Para obter mais informações sobre a definição de configurações de hardware de comunicação para uma localização específica, consulte "Hardware de Comunicação" na página 72.

Determine se deseja habilitar ou desabilitar a configuração global de cada dispositivo de hardware de comunicação listado:

- **1394 (FireWire):** Controla a porta de acesso do FireWire* no ponto de extremidade.
- **IrDA:** Controla a porta de acesso de infravermelho no ponto de extremidade.
- **Bluetooth:** Controla a porta de acesso do Bluetooth* no ponto de extremidade.
- **Serial/Paralela:** Controla o acesso a portas seriais e paralelas no ponto de extremidade.

Controle de Dispositivo de Armazenamento

Os controles de dispositivo de armazenamento definem as configurações de dispositivo de armazenamento padrão da política. Isso inclui especificar se os dispositivos externos de armazenamento de arquivos terão permissão para ler ou gravar arquivos, funcionarão no estado apenas leitura ou poderão ser completamente desabilitados. Quando desabilitados, esses dispositivos não podem recuperar dados do ponto de extremidade. No entanto, o disco rígido e todas as unidades de rede permanecem acessíveis e operacionais.

O Controle de Dispositivo de Armazenamento do ZENworks Endpoint Security Management não é permitido quando a Solução de Criptografia de Armazenamento está ativada.

Observa o: Você pode definir os controles de dispositivo de armazenamento globalmente na guia *Configurações de Política Global* ou pode defini-los para localizações individuais na guia *Localizações*.

Para definir os controles de dispositivo de armazenamento globalmente, clique na guia *Configurações de Política Global*, expanda *Configurações Globais* na árvore e clique em *Controle de Dispositivo de Armazenamento*.

Para definir os controles de dispositivo de armazenamento para uma localização específica, clique na guia *Localizações*, expanda a localização desejada na árvore e clique em *Controle de Dispositivo de Armazenamento*. Para obter mais informações, consulte "Hardware de Comunicação" na página 72.

Controle de Dispositivo de Armazenamento é dividido nas seguintes categorias:

- **CD/DVD:** Controla todos os dispositivos listados em *Unidades de DVD/CD-ROM* do Gerenciador de Dispositivos do Windows.
- **Armazenamento Removível:** Controla todos os dispositivos registrados como dispositivos de armazenamento removíveis em *Unidades de disco* do Gerenciador de Dispositivos do Windows.
- **Unidade de Disquete:** Controla todos os dispositivos listados em *Unidades de disquete* do Gerenciador de Dispositivos do Windows.
- **Dispositivos Preferidos:** Permite apenas os dispositivos de armazenamento removíveis listados na janela Controle de Dispositivo de Armazenamento. Todos os outros dispositivos registrados como dispositivos de armazenamento removíveis não são permitidos.

Dispositivos de armazenamento fixo (unidades de disco rígido) e unidades de rede (quando disponíveis) são sempre permitidos.

Para definir o padrão de política dos dispositivos de armazenamento, selecione nas listas suspensas a configuração global para ambos os tipos:

- **Habilitar:** O tipo de dispositivo é permitido por padrão.
- **Desabilitar:** O tipo de dispositivo não é permitido. Quando tentam acessar arquivos em um dispositivo de armazenamento definido, os usuários recebem uma mensagem de erro do sistema operacional ou do aplicativo que tenta acessar o dispositivo de armazenamento local, indicando que a ação falhou
- **Apenas Leitura:** O tipo de dispositivo é definido como Apenas Leitura. Quando tentam gravar no dispositivo, os usuários recebem uma mensagem de erro do sistema operacional ou do aplicativo que tenta acessar o dispositivo de armazenamento local, indicando que a ação falhou

---

Observa o: Se desejar desabilitar unidades de CD-ROM ou unidades de disquete em um grupo de pontos de extremidade ou se desejar definir essas unidades como Apenas Leitura, verifique se as opções *Dispositivos: restringir acesso ao CD-ROM apenas aos usuários com logon local* e *Dispositivos: restringir acesso ao disquete apenas aos usuários com logon local* estão definidas como Desabilitado nas Configurações de Segurança Local (passadas por um objeto Política do

grupo de serviços de diretório). Para verificar isso, abra o objeto Política de Grupo ou a opção Ferramentas Administrativas em uma máquina. Examine Configurações de Segurança Local - Opções de Segurança e verifique se ambos os dispositivos estão desabilitados. Desativado é o padrão.

As seções a seguir contêm mais informações:

- "Dispositivos Preferidos" na página 54
- "Importando listas de dispositivos" na página 55

Dispositivos Preferidos

É possível adicionar Dispositivos de Armazenamento Removíveis Preferidos a uma lista permitindo apenas o acesso aos dispositivos autorizados quando a configuração global é usada em um local. Os dispositivos adicionados à lista devem ter um número de série.

Para listar os dispositivos preferidos:

1. Insira o dispositivo na porta USB da máquina em que o Console de Gerenciamento está instalado.
2. Quando o dispositivo estiver pronto, clique no botão *Explorar*. Se o dispositivo tiver um número de série, sua descrição e seu número de série serão exibidos na lista.
3. Selecione uma configuração na lista suspensa (a configuração *Dispositivo Removível Global* não se aplica a essa política):
   - **Habilitado:** Os dispositivos da lista de preferidos recebem autorização total para leitura/gravação; todos os outros dispositivos USB e de armazenamento externos são desabilitados.
   - **Apenas Leitura:** Os dispositivos da lista de preferidos recebem autorização apenas leitura; todos os outros dispositivos USB e de armazenamento externos são desabilitados.

Repita essa etapas para cada dispositivo permitido na política. A mesma configuração será aplicada a todos os dispositivos.

Observa o: As configurações de Controle de Dispositivo de Armazenamento baseadas em localização anulam as configurações globais. Por exemplo, você pode definir que todos os dispositivos de armazenamento externos sejam permitidos no local de trabalho e que apenas o padrão global seja permitido nas outras localizações, limitando os usuários aos dispositivos presentes na lista de preferidos.

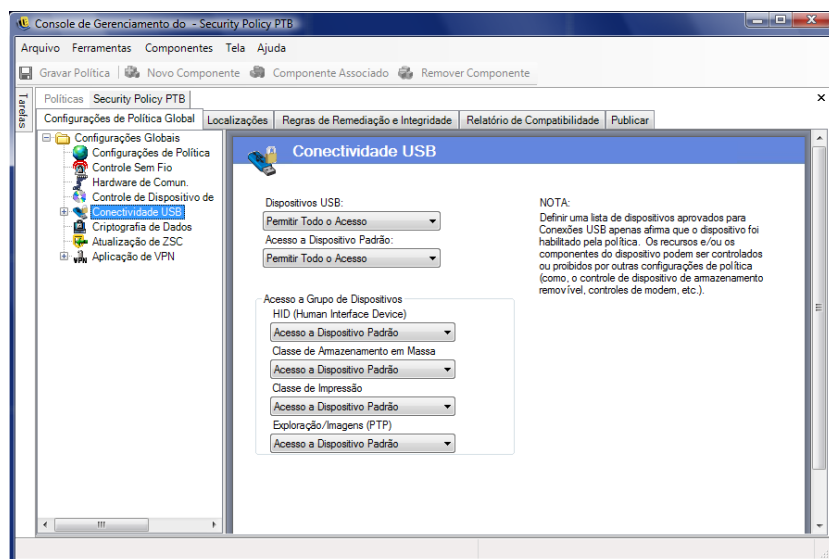
Importando listas de dispositivos

O aplicativo Scanner da Unidade USB da Novell gera uma lista de dispositivos e dos respectivos números de série (Seção 1.11, “Scanner da Unidade USB” na página 42). Para importar essa lista, clique em *Importar* e navegue até ela. A lista preenche os campos *Descrição* e *Número de Série*.

Conectividade USB

Todos os dispositivos que se conectam por meio do barramento USB podem ser permitidos ou negados pela política. Esses dispositivos podem ser explorados na política a partir do relatório de inventário de Dispositivos USB. Também é possível explorar todos os dispositivos conectados à máquina no momento. Esses dispositivos podem ser filtrados por fabricante, nome do produto, número de série, tipo, etc. Para fins de suporte, o administrador pode configurar a política para aceitar um conjunto de dispositivos por tipo de fabricante (por exemplo, todos os dispositivos HP são permitidos) ou por tipo de produto (por exemplo, todos os dispositivos USB de interface com o usuário, como mouse e teclado, são permitidos). Além disso, dispositivos individuais podem ser permitidos para impedir que dispositivos sem suporte sejam inseridos na rede (por exemplo, nenhuma impressora é permitida, exceto esta).

Para acessar esse controle, clique na guia *Configurações de Política Global* e, em seguida, clique em *Conectividade USB* na árvore de política à esquerda.

Figura 2-1 *Página Conectividade USB.*

Primeiramente, o acesso é avaliado com base na ativação ou na desativação do barramento. Isso é determinado pela configuração *Dispositivos USB*. Se a configuração estiver definida como *Desabilitar Todo o Acesso*, o dispositivo será desabilitado e a avaliação, interrompida. Se a configuração estiver definida como *Permitir Todo o Acesso*, o cliente continuará a avaliação e procurará por correspondências de filtro. Como acontece com muitos outros campos do Console de Gerenciamento do ZENworks, quando for definido em uma localização, o valor de *Dispositivos USB* também poderá ser definido para *Aplicar Configurações Globais*, e o valor global desse campo será usado.

O cliente reúne os filtros aplicados a partir da política, com base na localização e nas configurações globais. Em seguida, o cliente agrupa os filtros com base no acesso aos seguintes grupos:

- **Sempre Bloquear:** Sempre bloquear o dispositivo. Essa configuração não pode ser anulada.
- **Sempre Permitir:** Sempre permitir acesso, a menos que o dispositivo corresponda a um filtro *Sempre Bloquear*.
- **Bloquear:** Bloquear acesso, a menos que o dispositivo corresponda a um filtro *Sempre Permitir*.
- **Permitir:** Permitir acesso, a menos que o dispositivo corresponda a um filtro *Sempre Bloquear* ou *Bloquear*.
- **Acesso Padrão de Dispositivo:** Forneça ao dispositivo o mesmo nível de acesso de *Acesso Padrão de Dispositivo*, caso nenhuma outra correspondência seja encontrada.

Os dispositivos são avaliados em relação a cada grupo na ordem mencionada acima (primeiramente o grupo *Sempre Bloquear*; em seguida, o grupo *Sempre Permitir*; e assim por diante). Quando um dispositivo corresponde a pelo menos um filtro de um grupo, o acesso a ele é definido de acordo com o nível e as interrupções de avaliação equivalentes. Se o dispositivo for avaliado em relação a todos os filtros e nenhuma correspondência for encontrada, o nível *Acesso Padrão de Dispositivo* será aplicado.

O Acesso de Dispositivo definido na área *Acesso de Grupo de Dispositivos* é levado em consideração juntamente com todos os outros filtros usados na localização. Para isso, são gerados filtros correspondentes para cada agrupamento quando a política é publicada para o cliente. Estes são os filtros:

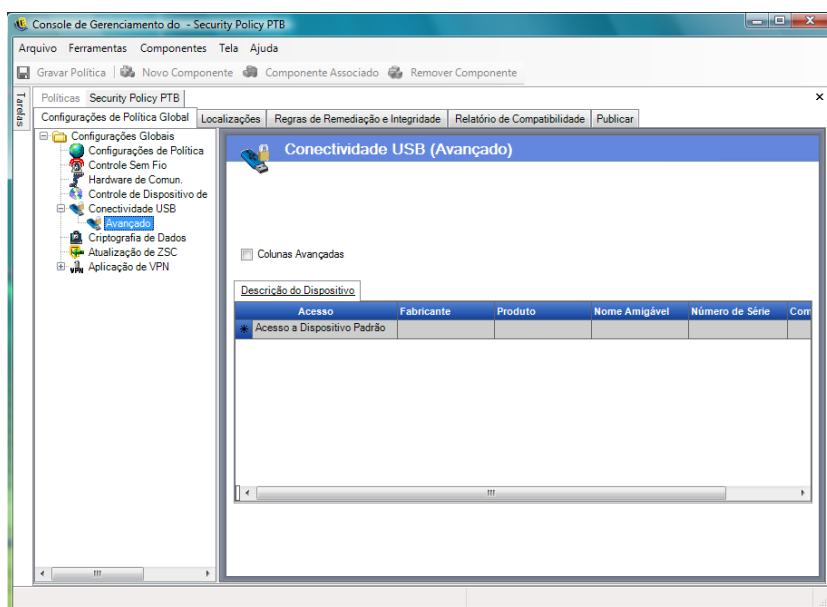
Acesso a Grupo de Dispositivos:	Filtro:
Dispositivo de Interface com o Usuário (HID)	A "Classe do Dispositivo" é igual a 3.
Classe do Armazenamento em Massa	A "Classe do Dispositivo" é igual a 8.
Classe da Impressão	A "Classe do Dispositivo" é igual a 7.
Exploração/Criação de Imagens (PTP)	A "Classe do Dispositivo" é igual a 6.

Avançado

Na maior parte das situações, os quatro grupos de dispositivos listados na página Conectividade USB (Dispositivo de Interface com o Usuário, Classe do Armazenamento em Massa, Classe da Impressão e Exploração/Criação de Imagens) são suficientes para permitir ou negar acesso à maioria dos dispositivos USB. Se houver algum dispositivo que não possa ser registrado em um desses grupos, você poderá definir configurações na página Avançado de Conectividade USB. Você

também poderá usar as configurações da página Avançado para fornecer acesso de lista de permissões a determinados dispositivos, mesmo que o acesso possa ser negado devido às configurações contidas na página Conectividade USB.

Para acessar as opções da página Avançado de Conectividade USB, na árvore *Configurações Globais*, clique no sinal de adição ao lado de *Conectividade USB* e, em seguida, clique em *Avançado*. Você pode usar o relatório de auditoria do Dispositivo USB como modo de obter todas as informações que possam ser usadas na página Avançado de Controle de Conectividade USB.

Figura 2-2 *Página Avançado de Conectividade USB.*

As colunas padrão incluem o seguinte:

- **Acesso:** Passe o mouse sobre *Acesso Padrão de Dispositivo* e especifique um nível de aceso:
  - **Sempre Bloquear:** Sempre bloquear o dispositivo. Essa configuração não pode ser anulada.
  - **Sempre Permitir:** Sempre permitir acesso, a menos que o dispositivo corresponda a um filtro *Sempre Bloquear*.
  - **Bloquear:** Bloquear acesso, a menos que o dispositivo corresponda a um filtro *Sempre Permitir*.
  - **Permitir:** Permitir acesso, a menos que o dispositivo corresponda a um filtro *Sempre Bloquear* ou *Bloquear*.
  - **Acesso Padrão de Dispositivo:** Forneça ao dispositivo o mesmo nível de acesso de *Acesso Padrão a Dispositivo*, caso nenhuma outra correspondência seja encontrada.
- **Fabricante:** Clique na coluna *Fabricante* e digite o nome do fabricante a ser incluído no filtro (Canon, por exemplo).
- **Produto:** Clique na coluna *Produto* e digite o nome do produto a ser incluído no filtro.
- **Nome Amigável:** Clique na coluna *Nome Amigável* e digite o nome amigável do dispositivo a ser incluído no filtro.

- **Número de Série:** Clique na coluna *Número de Série* e digite o número de série do dispositivo a ser incluído no filtro.
- **Comentário:** Clique na coluna *Comentário* e digite o comentário a ser incluído no filtro (Canon, por exemplo).

Clique na caixa *Colunas Avançadas* para adicionar as seguintes colunas: *Versão USB*, *Classe do Dispositivo, Subclasse do Dispositivo, Protocolo do Dispositivo, ID do Fornecedor, ID do Produto, Dispositivo BCD, ID do Dispositivo O/S* e *Classe do Dispositivo O/S*.

Os dispositivos disponibilizam um conjunto de atributos para o OS. O cliente cria correspondência para esses atributos nos campos exigidos pelo filtro. Para terem correspondência, todos os campos do filtro devem coincidir com um atributo fornecido pelo dispositivo. Se o dispositivo não fornecer um atributo ou um campo exigido pelo filtro, o filtro não encontrará correspondência.

Por exemplo, suponha que um dispositivo forneça os seguintes atributos: Fabricante: Acme, Classe: 8 e Número de Série: "1234".

O filtro: Classe == 8 corresponderá a esse dispositivo. O filtro: Produto == "Acme" não corresponderá, pois o dispositivo não forneceu um atributo Produto ao OS.

Os seguintes campos têm correspondências de sub-strings: Fabricante, Produto e Nome Amigável. Todos os outros campos têm correspondências exatas.

O campo Número de Série (NS) USB só será exclusivo se considerado quando os seguintes campos forem especificados junto com o NS: Versão USB, ID do Fornecedor, ID do Produto e Dispositivo BCD.

Estes são os valores atuais válidos da versão USB (em decimais): 512 - USB 2,0; 272 - USB 1,1; 256 - USB 1,0.

As seções a seguir contêm mais informações:

- "Adicionando dispositivos manualmente" na página 58
- "Colocando um dispositivo na lista de permissões ou na lista negra com base no tipo de produto" na página 59

Adicionando dispositivos manualmente

O seguinte método permite que você preencha a lista a fim de permitir ou negar conectividade USB aos dispositivos:

Para adicionar um dispositivo manualmente:

1. Insira o dispositivo na porta USB da máquina em que o Console de Gerenciamento está instalado.
2. Quando o dispositivo estiver pronto, clique no botão *Explorar*. Se o dispositivo tiver um número de série, a Descrição e o Número de Série serão exibidos na lista.
3. Selecione uma configuração na lista suspensa (a configuração *Dispositivo Removível Global* não se aplica a essa política):
   - **Habilitar:** Os dispositivos da lista de preferidos recebem autorização completa de leitura/gravação; todos os outros dispositivos USB e de armazenamento externo são desabilitados
   - **Apenas Leitura:** Os dispositivos da lista de preferidos recebem autorização apenas leitura; todos os outros dispositivos USB e de armazenamento externo são desabilitados

Repita essas etapas para cada dispositivo permitido na política. A mesma configuração será aplicada a todos os dispositivos.

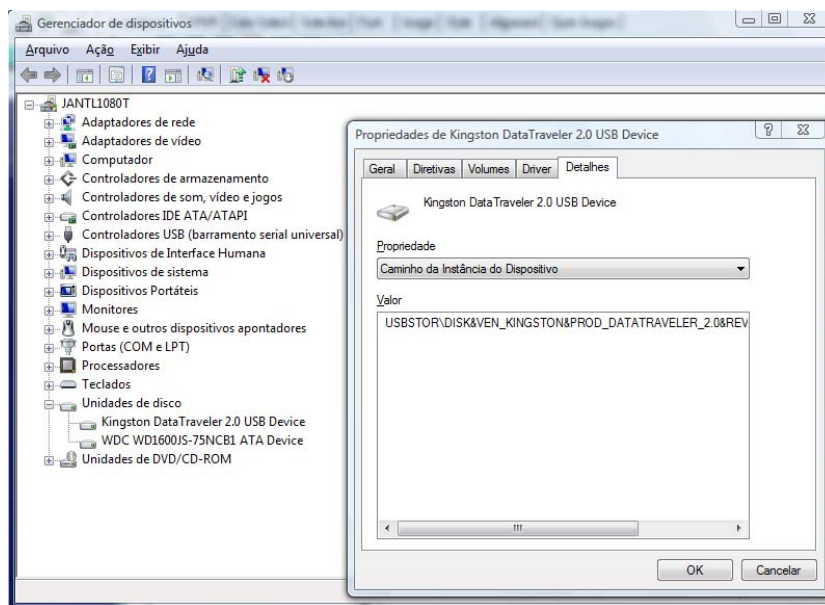
Colocando um dispositivo na lista de permissões ou na lista negra com base no tipo de produto

A seção a seguir descreve como colocar um dispositivo USB na lista de permissões ou na lista negra com base em seu tipo de produto.

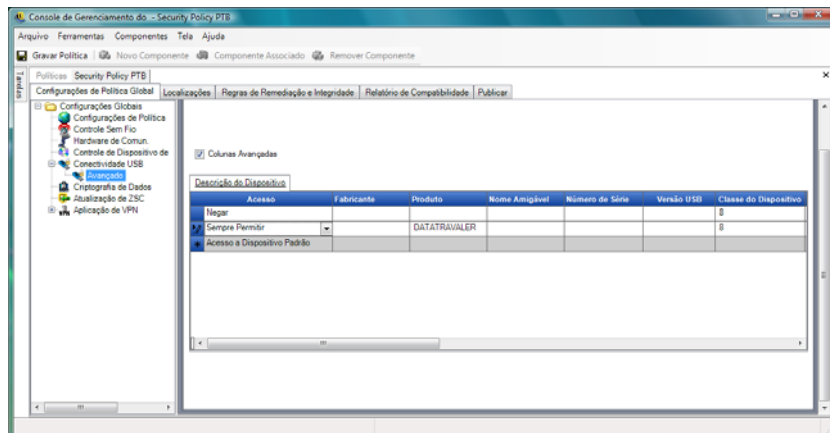
Observa o: O procedimento descrito a seguir é um exemplo de como você poderá encontrar o tipo de produto do seu dispositivo USB de armazenamento removível. Dependendo das informações fornecidas pelo fabricante do dispositivo, o procedimento pode não funcionar. Você pode usar o relatório de auditoria do Dispositivo USB como modo de obter todas as informações que possam ser usadas na página Avançado de Controle de Conectividade USB.

Para determinar o tipo de produto de um dispositivo USB de armazenamento removível:

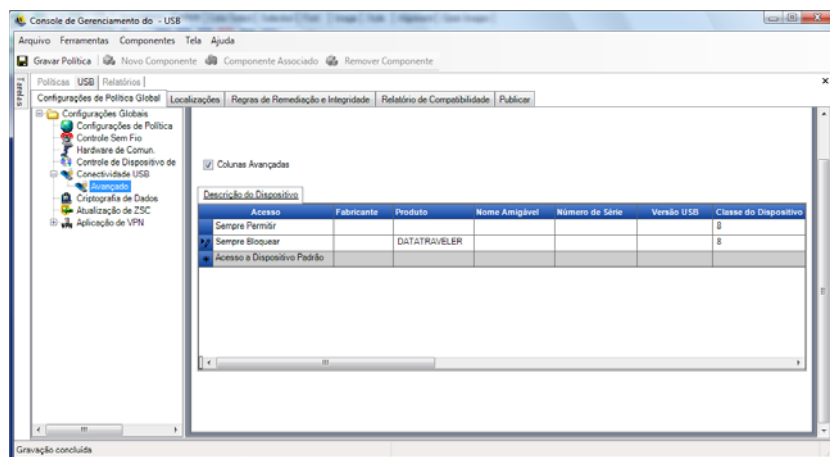
1. No Console de Gerenciamento de um computador com o Microsoft Windows, clique em *Gerenciador de Dispositivos*.
2. Clique no sinal de adição ao lado de *Unidades de disco* para expandir a árvore.
3. Clique o botão direito do mouse no dispositivo USB e, em seguida, clique em *Propriedades* para exibir a caixa de diálogo Propriedades do dispositivo.
4. Clique na guia *Detalhes* e selecione *Identificação de Instância de Dispositivo* na lista suspensa.

   O tipo de produto é listado após &PROD na Identificação de Instância de Dispositivo. No exemplo a seguir, DATATRAVELER é o tipo de produto.

Colocando um dispositivo USB na lista de permissões: Mantenha as configurações padrão da página Conectividade USB. Na página Avançada, crie duas linhas. Na primeira linha, especifique *Negar* na coluna *Acesso* e 8 na coluna *Classe do Dispositivo* (se *Classe do Dispositivo* não estiver

disponível, marque a caixa de seleção *Colunas Avançadas*). Na segunda linha, especifique *Sempre Permitir* na coluna *Acesso*, o tipo de produto (DATATRAVELER, neste exemplo) na coluna *Produto* e 8 na coluna *Classe do Dispositivo*.

A página Conectividade USB (Avançada) deve ter a seguinte aparência:

Agora, o dispositivo USB DATATRAVELER está na lista de permissões, o que significa que o ZENworks Endpoint Security Management concedeu acesso a ele e negou acesso a todos os outros dispositivos USB de armazenamento removível.

Colocando um dispositivo USB na lista negra: Mantenha as configurações padrão da página Conectividade USB. Na página Avançada, crie duas linhas. Na primeira linha, especifique *Sempre Permitir* na coluna *Acesso* e 8 na coluna *Classe do Dispositivo* (se *Classe do Dispositivo* não estiver disponível, marque a caixa de seleção *Colunas Avançadas*). Na segunda linha, especifique *Sempre Bloquear* na coluna *Acesso*, o tipo de produto (DATATRAVELER, neste exemplo) na coluna *Produto* e 8 na coluna *Classe do Dispositivo*.

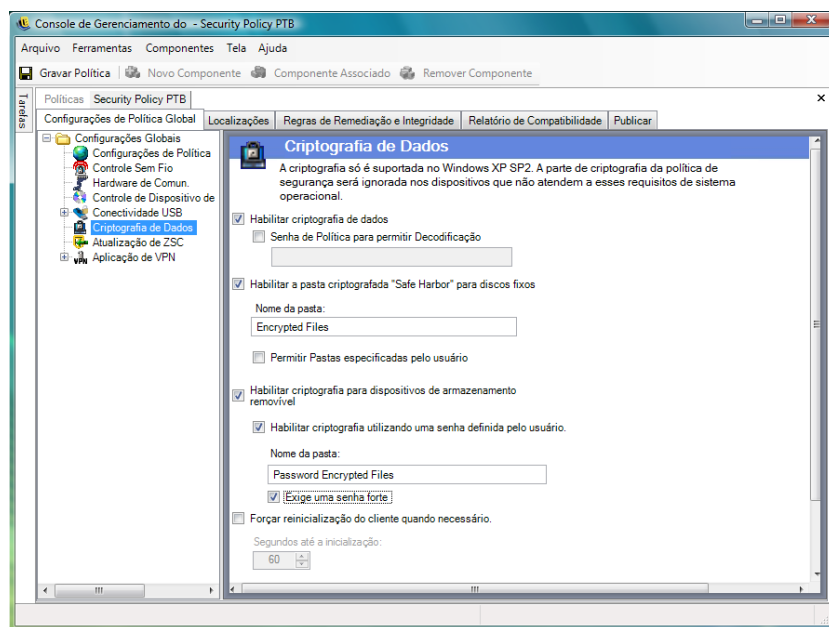
A página Conectividade USB (Avançada) deve ter a seguinte aparência:

Agora, o dispositivo USB DATATRAVELER está na lista negra, o que significa que o ZENworks Endpoint Security Management negou acesso a ele e concedeu acesso a todos os outros dispositivos USB de armazenamento removível.

Criptografia de Dados

A Criptografia de Dados determina se a criptografia de arquivos será aplicada no ponto de extremidade e o tipo de criptografia que estará disponível. Você pode criptografar os dados para permitir compartilhamento de arquivos (com proteção de senha) ou pode definir que os dados criptografados sejam lidos somente em computadores que executem a Solução de Criptografia de Armazenamento do ZENworks.

Observa o: A criptografia só é suportada no Windows XP SP2. A parte de criptografia da política de segurança é ignorada em dispositivos que não atendem a esse requisito de sistema operacional.

O Controle de Dispositivo de Armazenamento do ZENworks Endpoint Security Management não é permitido quando a Solução de Criptografia de Armazenamento do ZENworks está ativada.

Para acessar esse controle, clique na guia *Configurações de Política Global* e, em seguida, clique em *Criptografia de Dados* na árvore de política à esquerda.

Para ativar os controles individuais, clique na caixa de seleção *Permitir Criptografia de Dados*.

Observa o: As chaves criptográficas são distribuídas em todas as máquinas que recebem políticas do Serviço de Distribuição de Políticas, quer a criptografia de dados esteja ativada ou não. No entanto, esse controle instrui o ZENworks Security Client a ativar os drivers de criptografia para que os usuários possam ler arquivos enviados sem precisar do Utilitário de Decodificação de Arquivos. Consulte Seção 1.9, “Utilizando o Utilitário de Decodificação de Arquivos do ZENworks” na página 40 para obter mais detalhes.

Determine quais níveis de criptografia são permitidos por essa política:

- **Senha de política para permitir decodificação:** Especifique uma senha a ser inserida por todos os usuários que estiverem utilizando a política antes da decodificação de qualquer arquivo criptografado armazenado nas pastas `Safe Harbor`.

  Essa configuração é opcional. Deixe-a em branco se não desejar exigir senha.

- **Habilitar a pasta criptografada “Safe Harbor” para os discos fixos (volume que não é do sistema):** Gera uma pasta chamada `Arquivos Protegidos por Criptografia` na raiz dos volumes que não são do sistema no ponto de extremidade. Todos os arquivos colocados nessa pasta são criptografados e gerenciados pelo ZENworks Security Client. Os dados colocados nessa pasta são criptografados automaticamente e só podem ser acessados por usuários autorizados nessa máquina.

  Para mudar o nome da pasta, clique no campo *Nome da Pasta*, selecione o texto atual e especifique o nome desejado.

  - **Criptografar pasta “Meus Documentos” do usuário:** Marque essa caixa para definir a pasta `Meus Documentos` do usuário como uma pasta criptografada (complementando a pasta `Safe Harbor`). Só se aplica à pasta `Meus Documentos` local.
  - **Permitir pastas especificadas do usuário (volume que não é do sistema):** Marque essa caixa para permitir que os usuários selecionem as pastas do computador que deverão ser criptografadas. Só se aplica aos usuários locais; unidades de rede ou dispositivos de armazenamento removíveis não podem ser criptografados.

  Aviso: Antes de desabilitar a criptografia de dados, verifique se todos os dados armazenados nessas pastas foram extraídos pelo usuário e armazenados em outro local.

- **Habilitar criptografia para dispositivos de armazenamento removível:** Todos os dados gravados em dispositivos de armazenamento removíveis a partir de um ponto de extremidade protegido por essa política são criptografados. Os usuários que têm essa política em suas máquinas podem ler os dados; portanto, é possível realizar o compartilhamento de arquivos por meio de dispositivos de armazenamento removíveis em um grupo de políticas. Os usuários fora desse grupo de políticas não podem ler os arquivos criptografados na unidade e só podem acessar arquivos contidos na pasta `Arquivos Compartilhados` (se ativada) com uma senha fornecida.

  - **Habilitar criptografia por meio de uma senha definida pelo usuário:** Essa configuração permite que o usuário armazene arquivos da pasta `Arquivos Compartilhados` no dispositivo de armazenamento removível (a pasta é gerada automaticamente quando a configuração é aplicada). O usuário poderá especificar uma senha quando forem adicionados arquivos a essa pasta, que será usada pelos usuários que não estão no grupo de políticas atual para extrair os arquivos.

    Para mudar o nome da pasta, clique no campo *Nome da Pasta*, selecione o texto atual e especifique o nome desejado.

  - **Exigir senha forte:** Essa configuração força o usuário a definir uma senha forte para a Pasta de Arquivos Compartilhados. Uma senha forte deve ter:
    - sete caracteres ou mais
    - pelo menos um caractere de cada um destes quatro tipos:
      - letras maiúsculas de A a Z
      - letras minúsculas de A a Z
      - números de 0 a 9
      - pelo menos um caractere especial ~!@#$%^&*()+{}[]:;<>?,./

    Por exemplo: y9G@wb?

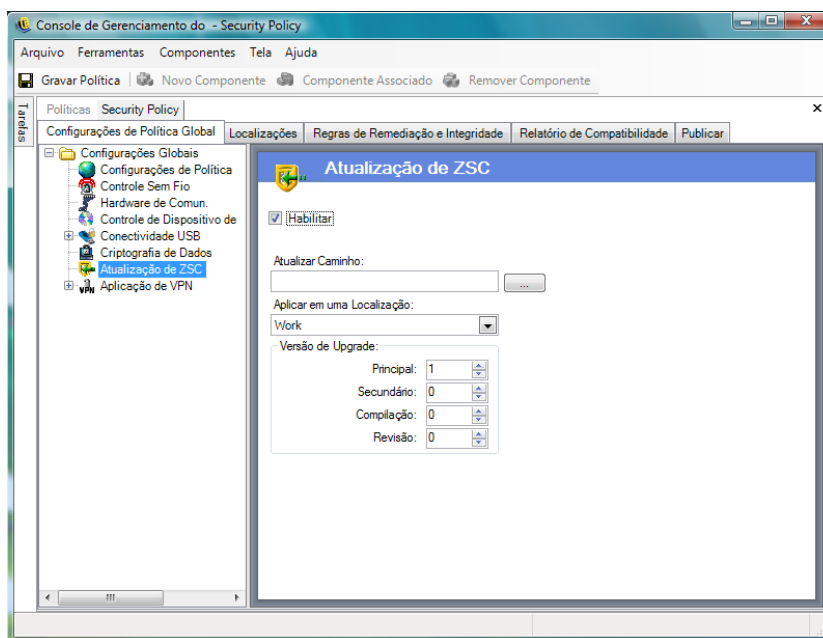
Aviso: Antes de desabilitar a criptografia de dados, verifique se todos os dados reunidos em dispositivos de armazenamento removível foram extraídos pelo usuário e armazenados em outro local.

- **Forçar reinicialização do cliente quando necessário:** Quando adicionada a uma política, a criptografia só se torna ativa quando o ponto de extremidade é reinicializado. Essa configuração força a reinicialização necessária exibindo um temporizador regressivo, que avisa que a máquina será reinicializada dentro do número de segundos especificado. O usuário tem esse tempo para gravar o trabalho antes que a máquina seja reinicializada.

  Reinicializações são necessárias quando a criptografia for ativada pela primeira vez em uma política e quando a unidade "Safe Harbor" ou a criptografia de armazenamento removível for ativada (caso seja ativada separadamente da ativação de criptografia). Por exemplo, quando uma política de criptografia é aplicada pela primeira vez, duas reinicializações são necessárias: uma para inicializar os drivers e outra para colocar safe harbors na criptografia. Se safe harbors adicionais forem selecionados subseqüentemente após a aplicação da política, apenas uma reinicialização será necessária para colocar safe harbor na política.

Atualização do ZSC

Patches para consertar pequenos defeitos no ZENworks Security Client são disponibilizados com as atualizações periódicas do ZENworks Endpoint Security Management. Em vez de fornecer um novo instalador, que precisa ser distribuído por MSI a todos os pontos de extremidade, a Atualização do ZENworks Security Client permite que o administrador dedique uma zona da rede que distribuirá patches de atualização a usuários finais quando eles se associarem a esse ambiente de rede.

Para acessar esse controle, clique na guia *Configurações de Política Global* e, em seguida, clique em *Atualização do ZSC* na árvore de política à esquerda.

Para permitir a distribuição simples e segura desses patches para todos os usuários do ZENworks Security Client:

1. Marque *Habilitar* para ativar a tela e a regra.

2. Especifique o local onde o ZENworks Security Client deverá procurar as atualizações.

   Devido às recomendações na etapa seguinte, o local associado ao ambiente da empresa (por exemplo, o local Trabalho) é o candidato recomendado.

3. Especifique o URI em que o patch foi armazenado.

   Ele precisa apontar para o arquivo de patch, que pode ser o arquivo setup.exe para o ZENworks Security Client ou um arquivo MSI criado com base no arquivo .exe. Por motivos de segurança, é recomendável que esses arquivos sejam armazenados em um servidor seguro por trás do firewall corporativo.

4. Especifique as informações de versão desse arquivo nos campos fornecidos.

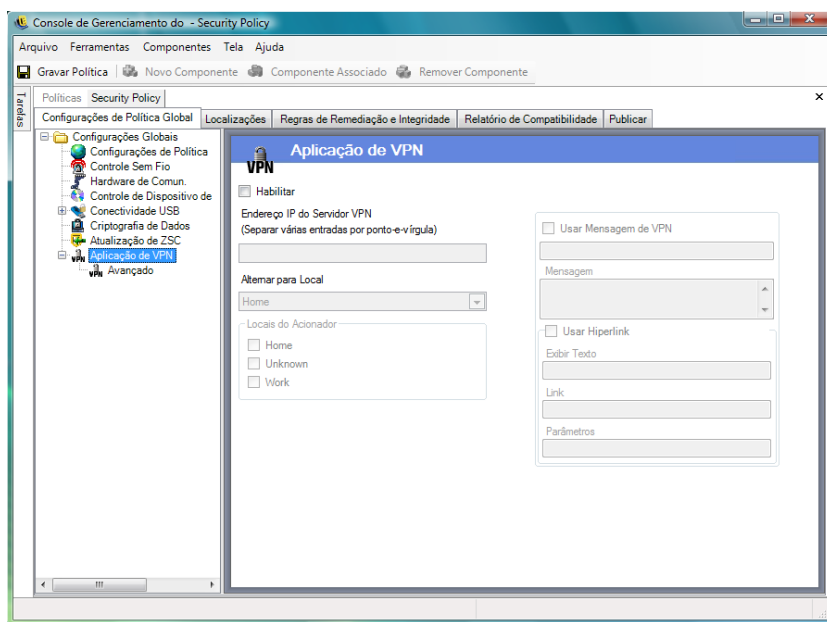
   Para encontrar as informações de versão, instale o ZENworks Security Client e abra a caixa de diálogo Sobre (consulte o *Guia de Instalação do ZENworks Endpoint Security Management* para obter detalhes). O número de versão do `STEngine.exe` é o número de versão a ser usado nos campos.

Cada vez que o usuário entra no local designado, o ZENworks Security Client verifica se há uma atualização no URI que corresponda a esse número de versão. Se houver uma atualização disponível, o ZENworks Security Client fará download dessa versão e a instalará.

Aplicação de VPN

Essa regra força o uso de um SSL ou de uma VPN (Virtual Private Network) baseada no cliente. Geralmente, essa regra é aplicada em pontos ativos sem fio, permitindo que o usuário se associe e se conecte à rede pública. Nesse momento, a regra tenta estabelecer a conexão VPN e, em seguida, alterna o usuário para uma configuração de firewall e localização definida. Todos os parâmetros ficam a critério do administrador. Todos os parâmetros anulam as configurações de políticas existentes. O componente Aplicação de VPN exige que o usuário seja conectado a uma rede antes da inicialização.

Observa o: Esse recurso só está disponível na instalação do ZENworks Endpoint Security Management e não pode ser usado para políticas de segurança UWS.

Para acessar esse controle, clique na guia *Configurações de Política Global* e, em seguida, clique em *Aplicação de VPN* na árvore de política à esquerda.

Para usar a regra Aplicação de VPN, é preciso que existam pelo menos duas localizações.

Para adicionar a imposição de VPN a uma política de segurança nova ou existente:

1. Selecione *Habilitar* para ativar a tela e a regra.
2. Especifique os endereços IP do servidor VPN no campo fornecido. Se forem especificados vários endereços, separe-os com ponto-e-vírgula (por exemplo: 10.64.123.5;66.744.82.36).
3. Na lista suspensa, selecione *Localização para Alternação*.

   É a localização para onde o ZENworks Security Client é alternado quando a VPN é ativada. Essa localização deve conter algumas restrições e deve usar apenas uma única configuração de firewall restritiva como padrão.

   A configuração de firewall *Todos Fechados*, que fecha todas as portas TCP/UDP, é recomendável para a aplicação de VPN estrita. Essa configuração bloqueia as redes não autorizadas e o endereço IP da VPN atua como ACL para o servidor VPN e habilita a conectividade de rede.
4. Selecione as localizações acionadoras em que a regra de aplicação de VPN será usada. Para aplicação de VPN estrita, a localização padrão Desconhecida deve ser usada para essa política. Depois da autenticação da rede, a regra de VPN é ativada e alternada para a Localização para Alternação designada.

   Observa o: A alternação de localização ocorre antes da conexão VPN e depois da autenticação da rede.

   ---
5. Forneça uma mensagem personalizada para o usuário a ser exibida quando a VPN for autenticada na rede. Para VPNs não-cliente, isso deve ser o suficiente.

   Para VPNs com um cliente, inclua um hiperlink que aponte para o cliente VPN.

   Exemplo: `C:\Arquivos de Programas\Cisco Systems\VPN Client\ipsecdialer.exe`

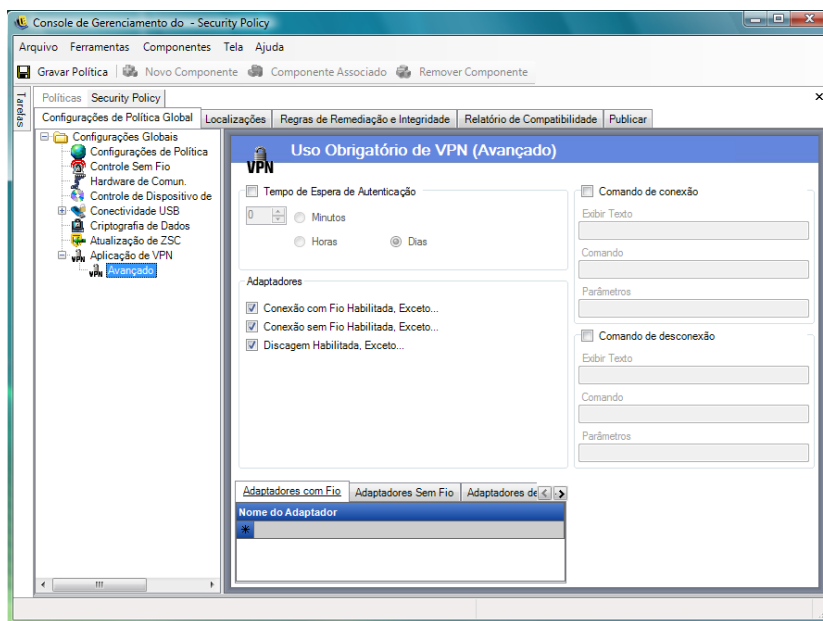
Esse link inicia o aplicativo, mas o usuário ainda precisa efetuar login. Um switch pode ser inserido no campo *Parâmetros*, ou um arquivo de lote, e não o executável do cliente, pode ser criado e apontado.

Observa o: Os clientes VPN que geram adaptadores virtuais (por exemplo, Cisco Systems* VPN Client 4.0) exibem a mensagem `A Política Foi Atualizada`. A política não foi atualizada; o ZENworks Security Client está simplesmente comparando o adaptador virtual a quaisquer restrições de adaptadores na política atual.

As configurações de Imposição de VPN padrão descritas acima tornam a conectividade VPN uma opção. O usuário recebe permissão de se conectar à rede atual, quer inicie sua VPN ou não. Para conhecer aplicações mais estritas, consulte Configurações de VPN Avançadas.

Configurações de VPN avançadas

Os controles avançados de VPN definem tempos de espera de autenticação para proteger contra falhas da VPN, conectar comandos para VPNs baseadas em cliente e usar controles de adaptador para controlar adaptadores que têm permissão de acesso à VPN.

Para acessar esse controle, clique na guia *Configurações de Política Global*, clique no símbolo "+" ao lado de *Aplicação de VPN* e, em seguida, clique em *Avançado* na árvore da política à esquerda.

É possível definir as seguintes configurações de aplicação de VPN avançada:

Tempo de Espera de Autenticação: Os administradores podem colocar o ponto de extremidade em uma configuração de firewall protegida (a configuração de firewall *Localização para Alternação*) para impedir falhas na conectividade da VPN. O *Tempo de Espera de Autenticação* é o tempo que o ZENworks Security Client aguarda para obter autenticação para o servidor VPN. Esse parâmetro deve ser definido como um valor superior a 1 minuto para permitir a autenticação em conexões lentas.

Comandos Conectar/Desconectar: Quando você usa o temporizador de autenticação, os comandos *Conectar* e *Desconectar* controlam a ativação da VPN baseada em cliente. Especifique o local do cliente VPN e os switches necessários nos campos *Parâmetros*. O comando Desconectar é opcional e é usado em clientes VPN que exigem que o usuário seja desconectado antes de efetuar logout da rede.

Observa o: Os clientes VPN que geram adaptadores virtuais (por exemplo, Cisco Systems VPN Client 4.0) exibem a mensagem `A Política Foi Atualizada` e podem sair temporariamente da localização atual. A política não foi atualizada; o ZENworks Security Client está simplesmente comparando o adaptador virtual a quaisquer restrições de adaptadores na política atual. Ao executar clientes VPN desse tipo, não utilize o hiperlink do comando Desconectar.

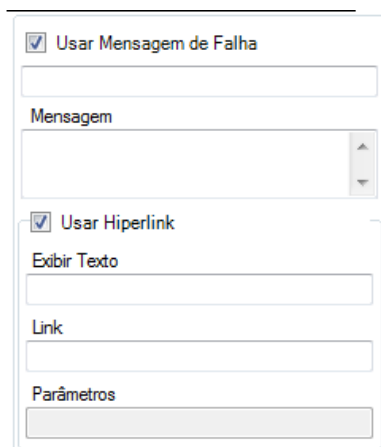
Adaptadores: Essa é basicamente uma política de adaptador resumida, específica da Aplicação de VPN.

Se um adaptador for selecionado (o que muda seu status para Habilitado, Exceto), ele (Sem Fio é específico do tipo de placa) será autorizado a ter conectividade com a VPN.

Os adaptadores contidos na lista de exceções não têm permissão para se conectar à VPN; todos os outros adaptadores desse tipo têm permissão de conectividade.

Se um adaptador não for selecionado (Habilitado, Exceto), apenas os adaptadores inseridos na lista de exceções terão permissão para se conectar à VPN. Todos os outros terão conectividade negada.

Esse controle pode ser usado para adaptadores incompatíveis com a VPN, por exemplo, ou adaptadores não suportados pelo departamento de TI.

Essa regra anula o conjunto de políticas de adaptador da localização para alternação.

Mensagens Personalizadas para o Usuário

As mensagens personalizadas para o usuário permitem que o administrador do ZENworks Endpoint Security Management crie mensagens que respondam diretamente às perguntas da política de segurança quando o usuário encontra restrições de segurança aplicadas pela política. As mensagens personalizadas também podem fornecer instruções específicas aos usuários. Os controles de mensagens para o usuário estão disponíveis em diversos componentes da política.

Para criar uma mensagem personalizada para o usuário:

1. Especifique um título para a mensagem. Esse título é exibido na barra de título da caixa de mensagem.
2. Especifique a mensagem. A mensagem está limitada a 1.000 caracteres.
3. Se for necessário um hiperlink, marque a caixa *Mostrar Hiperlinks* e especifique as informações solicitadas.

Observa o: Mudar uma mensagem ou um hiperlink em um componente compartilhado, mudará essa mensagem ou esse hiperlink em todas as outras instâncias do componente. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

Hiperlinks

Um administrador pode incorporar hiperlinks em Mensagens Personalizadas para o Usuário para ajudar a explicar políticas de segurança ou fornecer links para atualizações de software a fim de manter a conformidade com a integridade. Há hiperlinks disponíveis em diversos componentes de políticas. Um hiperlink de VPN pode ser criado para apontar para o executável do cliente VPN ou para um arquivo de lote que execute e conecte completamente o usuário à VPN (consulte "Aplicação de VPN" na página 64 para obter mais detalhes).

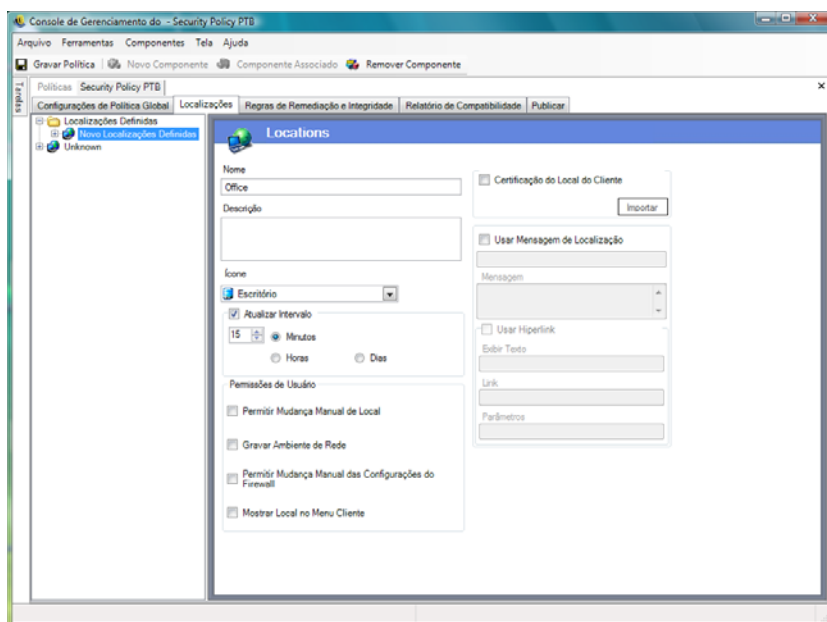
Para criar um hiperlink:

1. Especifique um nome para o link. Esse nome será exibido abaixo da mensagem. Além disso, esse nome é necessário para hiperlinks de VPN avançada.
2. Especifique o hiperlink.
3. Especifique os switches ou outros parâmetros do link.

Observa o: Mudar uma mensagem ou um hiperlink em um componente compartilhado, mudará essa mensagem ou esse hiperlink em todas as outras instâncias do componente. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

2.2.2 Localizações

As localizações são grupos de regras designadas a ambientes de rede. Esses ambientes podem ser definidos na política (consulte "Ambientes de Rede" na página 86) ou pelo usuário, quando permitido. É possível fornecer a cada localização configurações de segurança exclusivas, negando acesso a determinados tipos de rede e hardware em ambientes de rede mais hostis, e concedendo acesso mais amplo em ambientes confiáveis.

Para acessar os controles de Localização, clique na guia *Localizações*.

As seções a seguir contêm mais informações:

- "Sobre localizações" na página 70
- "Hardware de Comunicação" na página 72
- "Controle de Dispositivo de Armazenamento" na página 74
- "Configurações de Firewall" na página 76
- "Ambientes de Rede" na página 86
- "Conectividade USB" na página 88
- "Gerenciamento de Wi-Fi" na página 90
- "Segurança Wi-Fi" na página 93

Sobre localizações

É possível configurar os seguintes tipos de localização:

A Localização Desconhecida: Todas as políticas têm uma localização Desconhecida padrão. Essa é a localização para a qual o ZENworks Security Client alternará os usuários quando eles saírem de um ambiente de rede conhecido. Essa localização Desconhecida é exclusiva de cada política e não está disponível como um componente compartilhado. Os Ambientes de Rede não podem ser definidos nem gravados para essa localização.

Para acessar os controles de Localização Desconhecida , clique na guia *Localizações* e clique na localização *Desconhecida* na árvore da política à esquerda.

Localizações Definidas: Você pode criar novas localizações definidas para a política ou pode associar localizações existentes (aquelas criadas para outras políticas).

Para criar uma nova localização:

1 Clique em *Localizações Definidas* e, em seguida, clique no botão *Novo Componente* na barra de ferramentas.

2 Dê um nome para a localização e forneça uma descrição.

3 Defina as configurações de localização:

Ícone: Selecione um ícone de localização para fornecer ao usuário uma dica visual que facilite a identificação da localização atual. O ícone de localização é exibido na barra de tarefas da área de notificação. Use a lista suspensa para ver e selecionar um dos ícones de localização disponíveis.

Intervalo de Atualização: Especifique uma configuração para determinar a freqüência com que o ZENworks Security Client verificará se há uma atualização de política quando entrar nessa localização. A freqüência é definida em minutos, horas ou dias. Se você desmarcar esse parâmetro, o ZENworks Security Client não verificará se há atualizações nessa localização.

Permissões de Usuário: Especifique as permissões do usuário:

- **Permitir Mudança de Localização Manual:** Permite que o usuário entre e saia dessa localização. Para localizações não gerenciadas (pontos ativos, aeroportos, hotéis, etc.), essa permissão deve ser concedida. Em ambientes controlados, onde os parâmetros de rede são conhecidos, essa permissão pode ser desabilitada. O usuário não poderá entrar nem sair de nenhuma localização se essa permissão estiver desabilitada. O ZENworks Security Client confiará nos parâmetros do ambiente de rede da localização.
- **Gravar Ambiente de Rede:** Permite que o usuário grave o ambiente de rede nessa localização para poder realizar uma alternação automática para a localização quando retornar. Essa configuração é recomendada para todas as localizações de alternação do usuário. É possível gravar vários ambientes de rede para uma única localização. Por exemplo, se uma Localização definida como Aeroporto fizer parte da política atual, cada aeroporto visitado pelo usuário poderá ser gravado como um ambiente de rede para essa localização. Dessa maneira, um usuário móvel pode retornar a um ambiente de aeroporto gravado, pois o ZENworks Security Client alternará automaticamente para a localização Aeroporto e aplicará as configurações de segurança definidas. Um usuário poderá, claro, mudar para uma localização e não gravar o ambiente.
- **Permitir Mudanças Manuais de Configurações de Firewall:** Permite que o usuário mude as configurações de firewall.
- **Mostrar Localização no Menu do Cliente:** Permite que a localização seja exibida no menu do cliente. Se essa opção não for selecionada, a localização nunca será exibida.

Garantia de Localização de Cliente: Como as informações do ambiente de rede usadas para determinar uma localização podem ser falsificadas facilmente, o que expõe o ponto de extremidade a invasões, a opção de verificação criptográfica de uma localização pode ser acessada por meio do CLAS (Serviço de Garantia de Localização de Cliente). Esse serviço só é confiável em ambientes de rede total e exclusivamente controlados pela empresa. A adição da Garantia de Localização de Cliente a uma localização significa que as permissões e as configurações de firewall dessa localização podem ser definidas como menos restritivas, pois pressupõe-se que o ponto de extremidade esteja protegido atrás do firewall de rede.

O ZENworks Security Client usa uma porta fixa configurável pela empresa para enviar uma verificação para o Serviço de Garantia de Localização de Cliente. O Serviço de Garantia de Localização de Cliente decodifica o pacote e responde à verificação, provando a existência da chave privada que corresponde à chave pública. O ícone da barra de tarefas inclui uma marca de seleção, o que indica que o usuário está na localização correta.

O ZENworks Security Client só poderá alternar para a localização se puder detectar o servidor CLAS. Se o servidor CLAS não for detectado, mesmo se todos os outros parâmetros de rede corresponderem, o ZENworks Security Client permanecerá na localização Desconhecida para proteger o ponto de extremidade.

Para ativar o CLAS de uma localização, marque a caixa de seleção *Garantia de Localização de Cliente*, clique em *Importar* e, em seguida, procure e selecione o arquivo. A palavra Configurado é exibida quando a chave é importada com sucesso.

Esta opção não está disponível para a localização Desconhecida.

Usar Mensagem de Localização: Permite que uma mensagem personalizada para o usuário opcional seja exibida quando o ZENworks Security Client alterna para essa localização. Essa mensagem pode fornecer instruções para o usuário final e detalhes sobre restrições da política nessa localização, ou pode incluir um hiperlink para obter mais informações.

4 Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, "Notificação de erros" na página 106.

Para associar uma localização existente:

1 Clique em *Localizações Definidas* e, em seguida, clique no botão *Associar Componente* na barra de ferramentas.
2 Selecione as localizações desejadas na lista.
3 Se desejar, edite as configurações.

Observa o: Se você mudar as configurações de um componente compartilhado, todas as outras instâncias desse componente serão afetadas. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

---

4 Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, "Notificação de erros" na página 106.

Várias localização definidas (além das localizações simples Trabalho e Desconhecida) devem ser configuradas na política para oferecer ao usuário diversas permissões de segurança quando ele se conectar fora do firewall da empresa. Usar nomes de localização simples (por exemplo, restaurantes, aeroportos, residências) e fornecer dicas visuais por meio do ícone da barra de tarefas da localização ajudam o usuário a alternar paras as configurações de segurança apropriadas a cada ambiente de rede.

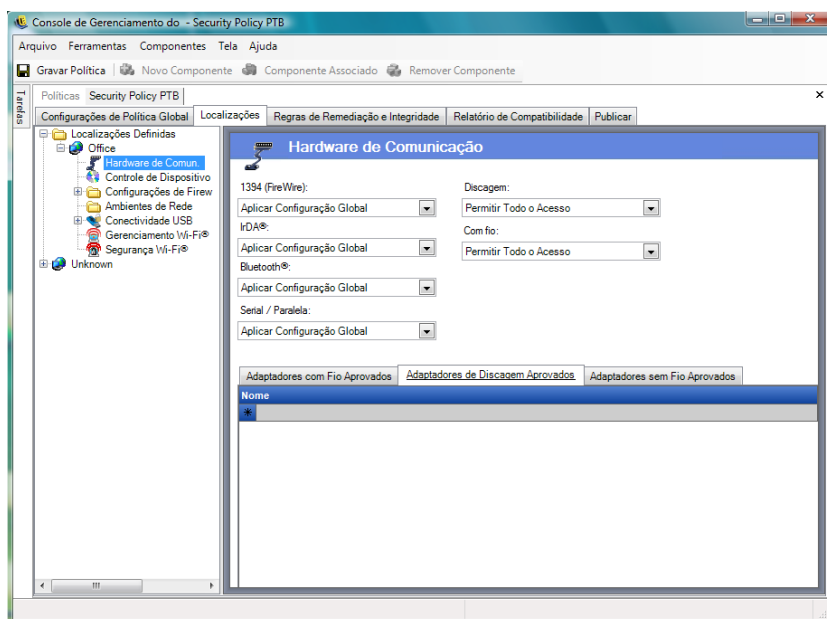
Hardware de Comunicação

As configurações de hardwares de comunicação controlam, por localização, que tipos de hardware podem se conectar nesse ambiente de rede.

Observa o: Você pode definir os controles de hardware de comunicação globalmente na guia *Configurações de Política Global* ou pode defini-los para localizações individuais na guia *Localizações*.

Para definir os controles de hardware de comunicação para uma localização específica, clique na guia *Localizações*, expanda a localização desejada na árvore e clique em *Hardware de Comunicação*.

ou

Para definir os controles de hardware de comunicação globalmente, clique na guia *Configurações de Política Global*, expanda *Configurações Globais* na árvore e clique em *Hardware de Comunicação*. Para obter mais informações, consulte "Hardware de Comunicação" na página 51.

Selecione a opção para habilitar, desabilitar ou aplicar a configuração global para cada dispositivo de hardware de comunicação listado:

- **1394 (FireWire):** Controla a porta de acesso do FireWire* no ponto de extremidade.
- **IrDA:** Controla a porta de acesso de infravermelho no ponto de extremidade.
- **Bluetooth:** Controla a porta de acesso do Bluetooth* no ponto de extremidade.
- **Serial/Paralela:** Controla o acesso a portas seriais e paralelas no ponto de extremidade.
- **Discagem:** Controla a conectividade do modem por localização. Essa opção não está disponível quando as configurações de hardware de comunicação são definidas globalmente na guia *Configurações de Política Global*.
- **Com Fio:** Controla a conectividade de placa de LAN por localização. Essa opção não está disponível quando as configurações de hardware de comunicação são definidas globalmente na guia *Configurações de Política Global*.

Habilitar permite acesso completo à porta de comunicação.

Desabilitar nega todo acesso à porta de comunicação.

Observa o: Adaptadores Wi-Fi são controlados globalmente ou desabilitados localmente por meio dos Controles de Segurança Wi-Fi. Para especificar os adaptadores por marca, use a lista Adaptador Sem Fio Aprovado.

Lista Adaptadores de Discagem Aprovados: O ZENworks Security Client pode bloquear todas as conexões, exceto as conexões de adaptadores de discagem (modems) aprovados e especificados. Por exemplo, um administrador pode implementar uma política que só permita uma determinada marca ou tipo de placa de modem. Isso reduz os custos associados ao uso de hardwares sem suporte pelos funcionários.

Lista Adaptadores Sem Fio Aprovados: O ZENworks Security Client pode bloquear todas as conexões, exceto as conexões de adaptadores sem fio aprovados e especificados. Por exemplo, um administrador pode implementar uma política que só permita uma determinada marca ou tipo de

placa sem fio. Isso reduz os custos de suporte associados ao uso de hardware sem suporte, além de melhorar o suporte e a aplicação de iniciativas de segurança baseadas em padrões IEEE, assim como LEAP, PEAP, WPA, TKIP e outros.

Utilizando o recurso AdapterAware:

O ZENworks Security Client recebe uma notificação sempre que um dispositivo de rede é instalado no sistema e determina se o dispositivo é autorizado ou não. Se o dispositivo não for autorizado, a solução desabilitará o driver do dispositivo, o que impedirá a utilização desse novo dispositivo e notificará o usuário sobre a situação.

Observa o: Quando um novo adaptador não autorizado (de discagem ou sem fio) instala pela primeira vez seus drivers no ponto de extremidade (via PCMCIA ou USB), o adaptador é mostrado como habilitado no Gerenciador de Dispositivos do Windows até que o sistema seja reinicializado, embora toda a conectividade de rede seja bloqueada.

Especifique o nome de cada adaptador permitido. É permitido usar nomes parciais de adaptadores. Os nomes de adaptadores podem ter no máximo 50 caracteres e fazem distinção entre maiúsculas e minúsculas. O sistema operacional Windows 2000 exige o nome do dispositivo para oferecer essa funcionalidade. Se nenhum adaptador for inserido, todos os adaptadores do tipo serão permitidos. Se apenas um adaptador for inserido, só esse adaptador será permitido nessa localização.

Observa o: Se o ponto de extremidade estiver em uma localização que defina apenas o SSID de um ponto de acesso como identificação de rede, o ZENworks Security Client alternará para essa localização antes de desabilitar o adaptador não autorizado. Se isso acontecer, use uma substituição de senha para fornecer uma alternação manual de localização.

Controle de Dispositivo de Armazenamento

Controles de dispositivo de armazenamento definem as configurações dos dispositivos de armazenamento padrão da política, onde todos os dispositivos de armazenamento de arquivos externos são autorizados a ler/gravar arquivos, funcionam em estado apenas leitura ou são totalmente desabilitados. Quando desabilitados, esses dispositivos não podem recuperar dados do ponto de extremidade. No entanto, o disco rígido e todas as unidades de rede permanecem acessíveis e operacionais.

O Controle de Dispositivo de Armazenamento do ZENworks Endpoint Security Management não é permitido quando a Solução de Criptografia de Armazenamento do ZENworks está ativada.

Observa o: Você pode definir os controles de dispositivo de armazenamento globalmente na guia *Configurações de Política Global* ou pode defini-los para localizações individuais na guia *Localizações*.

Para definir os controles de dispositivo de armazenamento para uma localização específica, clique na guia *Localizações*, expanda a localização desejada na árvore e clique em *Controle de Dispositivo de Armazenamento*.

ou

Para definir os controles de dispositivo de armazenamento globalmente, clique na guia *Configurações de Política Global*, expanda *Configurações Globais* na árvore e clique em *Controle de Dispositivo de Armazenamento*. Para obter mais informações, consulte "Controle de Dispositivo de Armazenamento" na página 52.

Controle de Dispositivo de Armazenamento é dividido nas seguintes categorias:

- **CD/DVD:** Controla todos os dispositivos listados em *Unidades de DVD/CD-ROM* do Gerenciador de Dispositivos do Windows.
- **Armazenamento Removível:** Controla todos os dispositivos registrados como dispositivos de armazenamento removíveis em *Unidades de disco* do Gerenciador de Dispositivos do Windows.
- **Unidade de Disquete:** Controla todos os dispositivos listados em *Unidades de disquete* do Gerenciador de Dispositivos do Windows.

Dispositivos de armazenamento fixo (unidades de disco rígido) e unidades de rede (quando disponíveis) são sempre permitidos.

Para definir o padrão de política dos dispositivos de armazenamento, selecione nas listas suspensas a configuração global para ambos os tipos:

- **Habilitar:** O tipo de dispositivo é permitido por padrão.
- **Desabilitar:** O tipo de dispositivo não é permitido. Quando tentam acessar arquivos em um dispositivo de armazenamento definido, os usuários recebem uma mensagem de erro do sistema operacional ou do aplicativo que tenta acessar o dispositivo de armazenamento local, indicando que a ação falhou
- **Apenas Leitura:** O tipo de dispositivo é definido como Apenas Leitura. Quando tentam gravar no dispositivo, os usuários recebem uma mensagem de erro do sistema operacional ou do aplicativo que tenta acessar o dispositivo de armazenamento local, indicando que a ação falhou

---

Observa o: Se desejar desabilitar unidades de CD-ROM ou unidades de disquete em um grupo de pontos de extremidade ou se desejar definir essas unidades como Apenas Leitura, verifique se as opções *Dispositivos: restringir acesso ao CD-ROM apenas aos usuários com logon local* e *Dispositivos: restringir acesso ao disquete apenas aos usuários com logon local* estão definidas

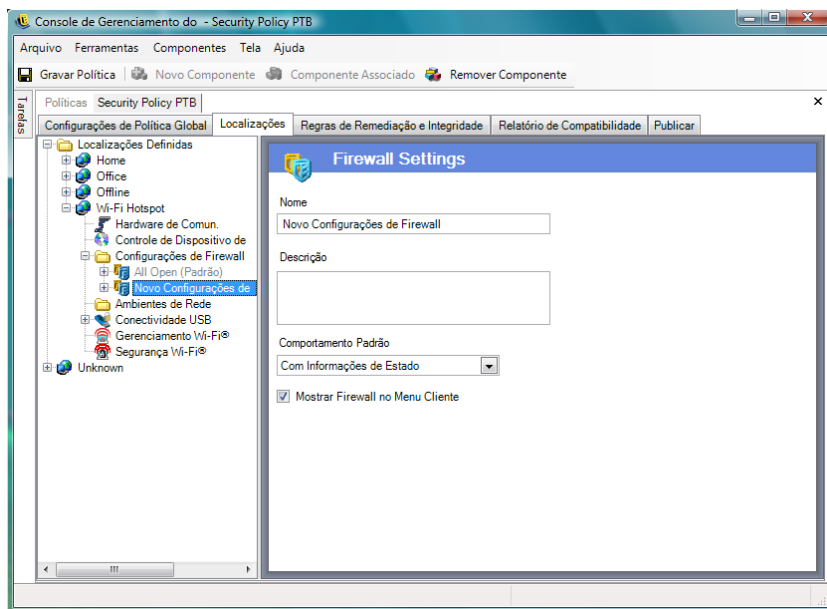
como Desabilitado nas Configurações de Segurança Local (passadas por um objeto Política do grupo de serviços de diretório). Para verificar isso, abra o objeto Política de Grupo ou a opção Ferramentas Administrativas em uma máquina. Examine Configurações de Segurança Local - Opções de Segurança e verifique se ambos os dispositivos estão desabilitados. Desativado é o padrão.

Configurações de Firewall

As Configurações de Firewall controlam a conectividade de todas as portas de rede, listas de Controle de Acesso, pacotes de rede (ICMP, ARP, etc.) e aplicativos que podem obter um soquete externo ou uma função quando a configuração de firewall é aplicada.

Observa o: Esse recurso só está disponível na instalação do ZENworks Endpoint Security Management e não pode ser usado para políticas de segurança UWS.

Para acessar esse controle, clique na guia *Localizações* e, em seguida, clique no ícone *Configurações de Firewall* na árvore da política à esquerda.

Cada componente de uma configuração de firewall é definido separadamente e somente a definição do comportamento padrão das portas TCP/UDP é obrigatória. Quando habilitada, essa configuração afeta todas as portas TCP /UDP. Portas individuais ou agrupadas podem ser criadas com uma configuração diferente.

Para criar uma nova configuração de firewall:

1. Selecione *Configurações de Firewall* na árvore de componentes e clique no botão *Novo Componente*.
2. Dê um nome para a configuração de firewall e forneça uma descrição.
3. Na árvore de componentes, clique o botão direito do mouse em *Portas TCP/UDP* e, em seguida, clique em *Adicionar Novas Portas TCP/UDP* para selecionar o comportamento padrão de todas as portas TCP/UDP.

   Portas e listas adicionais podem ser incluídas nas configurações de firewall e receber comportamentos exclusivos que anulem as configurações padrão.

   Por exemplo, o comportamento padrão de todas as portas é definido como Todos com Informações de Estado. Isso significa que as listas de portas para streaming media e navegação na Web são adicionadas à configuração de firewall. O comportamento da porta de streaming media é definido como Fechado e o da porta de navegação na Web é definido como Aberto. O tráfego de rede pelas portas TCP 7070, 554, 1755 e 8000 é bloqueado. O tráfego de rede pelas portas 80 e 443 fica aberto e visível na rede. Todas as outras portas operam em modo Com Informações de Estado e exigem que o tráfego seja solicitado primeiro.

   Para obter mais informações, consulte "Portas TCP/UDP" na página 78.
4. Clique o botão direito do mouse em *Listas de Controle de Acesso* e, em seguida, clique em *Adicionar Novas Listas de Controle de Acesso* para incluir endereços que possam precisar que tráfego não solicitado passe, independentemente do comportamento da porta atual.

   Para obter mais informações, consulte "Listas de Controle de Acesso" na página 82.
5. Clique o botão direito do mouse em *Controle de Aplicativos*e, em seguida, clique em *Adicionar Novos Controles de Aplicativos* para impedir que determinados aplicativos obtenham acesso à rede ou simplesmente impedir que sejam executados.

   Para obter mais informações, consulte "Controles de Aplicativo" na página 84.

6 Determine se o firewall deve ser exibido no menu do ZENworks Security Client (se essa opção não for selecionada, o usuário não verá a configuração do firewall).

7 Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, “Notificação de erros” na página 106.

Para associar uma configuração de firewall existente:

1 Selecione *Configurações de Firewall* na árvore de componentes e clique no botão *Associar Componente*.

2 Selecione as configurações de firewall desejadas na lista.

3 Se necessário, mude a configuração de comportamento padrão.

Observa o: Se você mudar as configurações de um componente compartilhado, todas as outras instâncias desse componente serão afetadas. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

---

4 Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, “Notificação de erros” na página 106.

É possível incluir várias configurações de firewall em uma única localização. Uma é definida como padrão e as restantes ficam disponíveis como opções de alternação do usuário. É útil ter várias configurações quando um usuário precisa utilizar com freqüência determinadas restrições de segurança em um ambiente de rede e ocasionalmente precisa que essas restrições sejam suspensas ou aumentadas por um breve período para, por exemplo, Broadcasts de ICMP.

As seguintes configurações de firewall são incluídas na instalação:

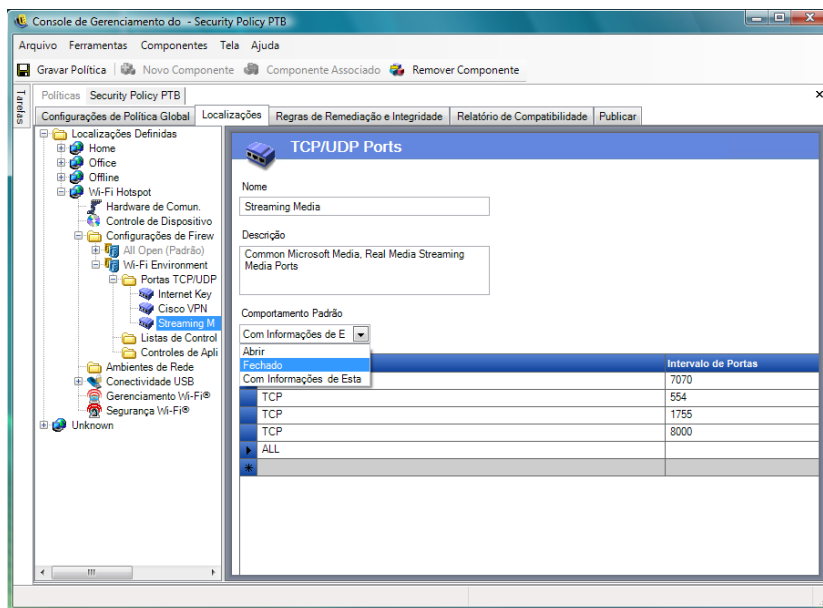
- **Tudo Adaptável:** Define todas as portas de rede como portas com informações de estado (todo tráfego de entrada na rede não solicitado é bloqueado e todo tráfego de saída da rede é permitido). Pacotes 802.1x e ARP são permitidos e todos os aplicativos de rede podem ter uma conexão de rede.
- **Tudo Aberto:** Define todas as portas de rede como abertas (todo tráfego da rede é permitido) e todos os tipos de pacote como permitidos. Todos os aplicativos de rede podem ter uma conexão de rede.
- **Tudo Fechado:** Fecha todas as portas de rede e restringe todos os tipos de pacote.

A configuração de firewall única, Todos Abertos, é definida como padrão em uma nova localização. Para definir outra configuração de firewall como padrão, clique o botão direito do mouse na configuração de firewall desejada e selecione *Definir como Padrão*.

Portas TCP/UDP

O principal método de proteção de dados do ponto de extremidade é o controle da atividade nas portas TCP/UDP. Esse recurso permite que você crie uma lista de portas TCP/UDP que serão tratadas de maneira exclusiva nessa configuração de firewall. As listas contêm uma coleção de portas e faixas de portas, além dos tipos de transporte, o que define a função da faixa.

Observa o: Esse recurso só está disponível na instalação do ZENworks Endpoint Security Management e não pode ser usado para políticas de segurança UWS.

Para acessar esse controle, clique na guia *Localizações*, clique no símbolo "+" ao lado de *Configurações de Firewall*, clique no símbolo “+” ao lado do firewall desejado e, em seguida, clique no ícone *Portas TCP/UDP* na árvore da política à esquerda.

Novas listas de portas TCP/UDP podem ser definidas com portas individuais ou como uma faixa de portas (1-100) para cada linha da lista.

Para criar uma nova configuração de porta TCP/UDP:

1. Na árvore de componentes, clique o botão direito do mouse em *Portas TCP/UDP* e, em seguida, clique em *Adicionar Novas Portas TCP/UDP*.
2. Dê um nome para a lista de portas e forneça uma descrição.
3. Selecione o comportamento da porta na lista suspensa:
   - **Aberto:** Todo tráfego de rede de entrada e de saída é permitido. Como todo tráfego de rede é permitido, a identidade do computador é mostrada na porta ou na faixa de portas.
   - **Fechado:** Todo tráfego de rede de entrada e de saída é bloqueado. Como todas as solicitações de identificação de rede são bloqueadas, a identidade do computador é ocultada da porta ou da faixa de portas.
   - **Com Informações de Estado:** Todo tráfego não solicitado de entrada na rede é bloqueado. Todo tráfego de saída da rede é permitido por essa porta ou por essa faixa de portas.
4. Para especificar o tipo de transporte, clique na seta para baixo na coluna*Tipo de Porta*:
   - TCP/UDP
   - Ether
   - IP
   - TCP
   - UDP

5. Insira portas e faixas de portas como:
   - Portas únicas
   - Uma faixa de portas com o primeiro número de porta, seguido de um traço, e o último número de porta

     Por exemplo, 1-100 adicionará todas as portas entre 1 e 100

     Visite as páginas Autoridade de Números Atribuídos (http://www.iana.org) na Internet para obter uma lista completa de portas e de tipos de transportes.
6. Clique em *Gravar Política*.

Para associar uma porta TCP/UDP existente a essa configuração de firewall:

1. Selecione *Portas TCP/UDP* na árvore de componentes e clique no botão *Associar Componente*.
2. Selecione as portas desejadas na lista.
3. Defina as configurações de comportamento padrão.

   Se você mudar as configurações de um componente compartilhado, todas as outras instâncias desse componente serão afetadas. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.
4. Clique em *Gravar Política*.

Diversos grupos de portas TCP/UDP foram reunidos e estão disponíveis durante a instalação:

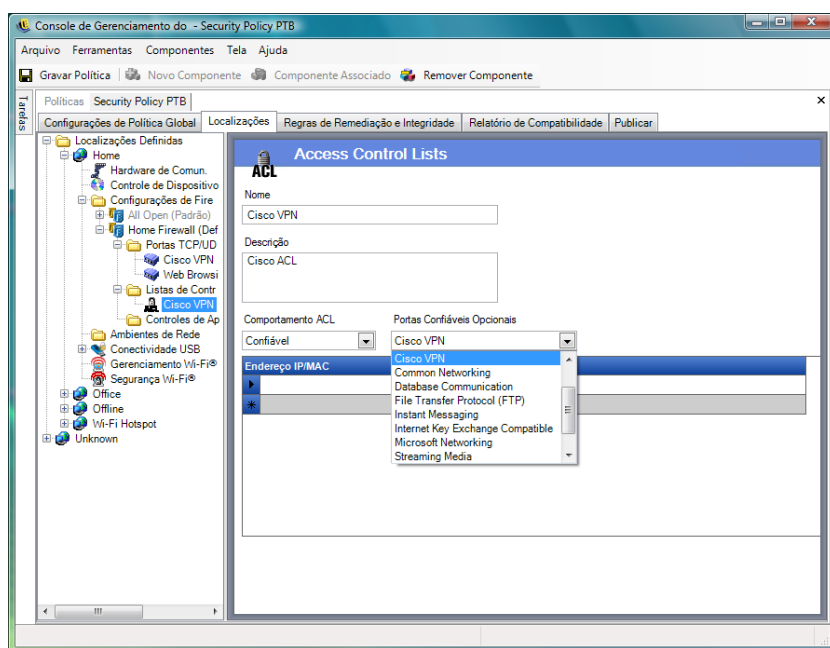
Nome	Descrição	Transporte	Valor
Todas as Portas	Todas as portas	Todos	1-65535
BlueRidge VPN	Portas usadas pelo cliente BlueRidge VPN	UDP	820
Cisco VPN	Portas usadas pelo cliente Cisco* VPN	IP	50,51
		UDP	500,4500
		UDP	1000-1200
		UDP	62514,62515,62517
		UDP	62519-62521
		UDP	62532,62524
Redes Comuns	Portas de rede normalmente necessárias para criar firewalls	TCP	53
		UDP	53
		UDP	67,68
		TCP	546, 547
		UDP	546, 547
		TCP	647, 847
		UDP	647, 847

Nome	Descrição	Transporte	Valor
Comunicação de Bancos de Dados	Portas de bancos de dados Microsoft*, Oracle*, Siebel*, Sybase*, SAP*	TCP	4100
		TCP	1521
		TCP	1433
		UDP	1444
		TCP	2320
		TCP	49998
		TCP	3200
		TCP	3600
FTP (File Transfer Protocol)	Porta FTP	TCP/UDP	21
Mensagens Instantâneas	Portas de mensagens instantâneas Microsoft, AOL*, Yahoo*	TCP	6891-6900
		TCP	1863,443
		UDP	1863,443
		UDP	5190
		TCP	6901
		UDP	6901
		TCP	5000-5001
		UDP	5055
		TCP	20000-20059
		UDP	4000
		TCP	4099
		TCP	5190
VPN Compatível com Intercâmbio de Chaves pela Internet	Portas usadas por clientes VPN compatíveis com o Internet Key Exchange	UDP	500
Rede Microsoft	Portas comuns de compartilhamento de arquivos/Active Directory*	TCP/UDP	135-139, 445
Portas Abertas	Portas abertas para este firewall	TCP/UDP	80
Streaming Media	Portas comuns da Microsoft e da Real Streaming Media	TCP	7070, 554, 1755, 8000
Navegação na Web	Portas comuns do browser da Web, incluindo SSL	Todos	80, 443

Listas de Controle de Acesso

Talvez alguns endereços precisem que o tráfego não solicitado passe, independentemente do comportamento da porta atual (por exemplo, servidor de backup do empreendimento, exchange server, etc.). Em instâncias em que o tráfego não solicitado precisa ser passado de e para servidores confiáveis, uma Lista de Controle de Acesso (ACL) resolve o problema.

Observa o: Esse recurso só está disponível na instalação do ZENworks Endpoint Security Management e não pode ser usado para políticas de segurança UWS.

Para acessar esse controle, clique na guia *Localizações*, clique no símbolo + ao lado de *Configurações de Firewall*, clique no símbolo + ao lado do firewall desejado, clique o botão direito do mouse em *Listas de Controle de Acesso* na árvore de política à esquerda e, em seguida, clique em *Adicionar Novas Listas de Controle de Acesso*.

Para criar uma nova configuração de ACL:

1. Na árvore de componentes, clique o botão direito do mouse em *Listas de Controle de Acesso* e, em seguida, clique em *Adicionar Novas Listas de Controle de Acesso*.
2. Dê um nome para a ACL e forneça uma descrição.
3. Especifique o endereço da ACL ou a macro.
4. Especifique o tipo de ACL:
    - **IP:** Nesse tipo, o endereço só pode conter 15 caracteres e esses caracteres devem ser números de 0 a 9 e pontos, como 123.45.6.189. Endereços IP também podem ser inseridos como uma faixa, como 123.0.0.0 - 123.0.0.255.
    - **MAC:** Nesse tipo, o endereço só pode conter 12 caracteres e esses caracteres devem ser números de 0 a 9 e letras de A a F (letras maiúsculas e minúsculas). Os caracteres devem ser separados por dois-pontos, como 00:01:02:34:05:B6.

5. Selecione a lista suspensa Comportamento da ACL e determine se as ACLs relacionadas devem ser definidas como *Confiável* (sempre permitidas, mesmo que todas as portas TCP/UDP sejam fechadas) ou *Não Confiável* (acesso bloqueado).
6. Se definir as ACLs como *Confiável*, selecione *Portas Confiáveis Opcionais (TCP/UDP) que a ACL usará*. Essas portas permitem todo tráfego de ACL, enquanto outras portas TCP/UDP mantêm suas configurações atuais. Se você selecionar *Nenhum*, a ACL poderá usar qualquer porta.
7. Clique em *Gravar Política*.

Para associar uma ACL ou uma macro existente a essa configuração de firewall:

1. Selecione *Lista de Controle de Acesso* na árvore de componentes e clique no botão *Associar Componente*.
2. Selecione as ACLs ou as macros na lista.
3. Defina as configurações de comportamento da ACL, conforme necessário.

   Observa o: Se você mudar as configurações de um componente compartilhado, todas as outras instâncias desse componente serão afetadas. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

4. Clique em *Gravar Política*.

Lista de macros de endereço de rede

Veja a seguir uma lista de macros especiais de Controle de Acesso. Essas macros podem ser associadas individualmente como parte de uma ACL em uma configuração de firewall.

Tabela 2-1 *Macros de endereço de rede*

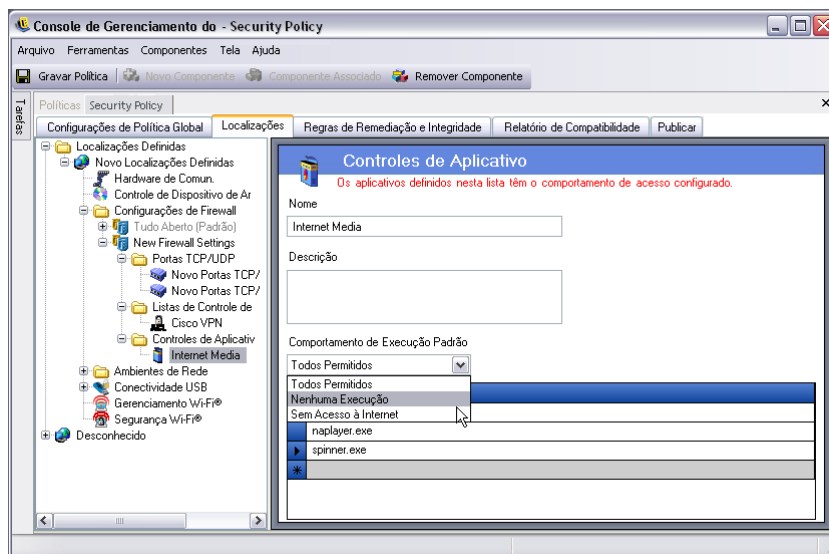
Macro	Descrição
[Arp]	Permite pacotes ARP (Protocolo de Resolução de Endereço). O termo *resolução de endereço* se refere ao processo de localização do endereço de um computador em uma rede. Para a resolução de endereço, use um protocolo no qual as informações são enviadas por um processo cliente em execução no computador local para um processo servidor em execução em um computador remoto. As informações recebidas pelo servidor permitem que ele identifique de forma exclusiva o sistema de rede para o qual o endereço foi solicitado e, desse modo, forneça o endereço necessário. O procedimento de resolução de endereço é concluído quando o cliente recebe uma resposta do servidor contendo o endereço solicitado.
[Icmp]	Permite pacotes ICMP (Protocolo de Mensagens de Controle da Internet). Os ICMPs são usados por roteadores, dispositivos intermediários ou hosts para comunicar atualizações ou informações sobre erros a outros roteadores, dispositivos intermediários ou hosts. As mensagens do ICMP são enviadas em diversas situações. Por exemplo, quando um datagrama não consegue atingir seu destino, quando o gateway não tem capacidade de buffer para encaminhar um datagrama e quando o gateway pode direcionar o host para enviar tráfego em uma rota mais curta.

Macro	Descrição
[IpMulticast]	Permite pacotes multicast IP. Multicast é uma tecnologia de conservação de largura de banda que reduz o tráfego, pois fornece um fluxo único de informações a milhares de destinatários em empresas e residências. Os aplicativos que usam multicast incluem videoconferências, comunicações corporativas e aprendizado à distância, bem como distribuição de software, cotações de ações e notícias. Os pacotes multicast podem ser distribuídos por meio de endereços Ethernet ou IP.
[EthernetMulticast]	Permite pacotes multicast Ethernet.
[IpSubnetBrdcast]	Permite pacotes broadcast de sub-rede. Broadcasts de sub-rede são usados para enviar pacotes a todos os hosts de redes configuradas como sub-redes, como super-redes ou como redes nonclassful. Todos os hosts de uma rede nonclassful escutam e processam pacotes enviados ao endereço de broadcast de sub-rede.
[Snap]	Permite pacotes codificados por SNAP.
[LLC]	Permite pacotes codificados por LLC.
[Allow8021X]	Permite pacotes 802.1X. Para superar deficiências em chaves WEP, a Microsoft e outras empresas utilizam 802.1x como método de autenticação alternativo. 802.1x é um controle de acesso a rede baseado em porta que usa o protocolo EAP ou certificados. Atualmente, a maioria dos fornecedores de placas sem fio e muitos fornecedores de ponto de acesso suportam o 802.1x. Essa configuração também permite pacotes de autenticação de protocolos LEAP e WPA.
[Gateway]	Representa o endereço de gateway padrão da configuração IP atual. Quando esse valor é inserido, o ZENworks Security Client permite todo tráfego de rede do gateway padrão da configuração IP atual como uma ACL confiável.
[GatewayAll]	O mesmo que [Gateway], mas para todos os gateways definidos.
[Wins]	Representa o endereço do servidor WINS padrão da configuração IP do cliente atual. Quando esse valor é inserido, o ZENworks Security Client permite todo tráfego de rede do servidor WINS padrão da configuração IP atual como uma ACL confiável.
[WinsAll]	O mesmo que [Wins], mas para todos os servidores WINS definidos.
[Dns]	Representa o endereço do servidor DNS padrão da configuração IP do cliente atual. Quando esse valor é inserido, o ZENworks Security Client permite todo tráfego de rede do servidor DNS padrão da configuração IP atual como uma ACL confiável.
[DnsAll]	O mesmo que [Dns], mas para todos os servidores DNS definidos.
[Dhcp]	Representa o endereço do servidor DHCP padrão da configuração IP do cliente atual. Quando esse valor é inserido, o ZENworks Security Client permite todo tráfego de rede do servidor DHCP padrão da configuração IP atual como uma ACL confiável.
[DhcpAll]	O mesmo que [Dhcp], mas para todos os servidores DHCP definidos.

Controles de Aplicativo

Esse recurso permite ao administrador impedir que aplicativos tenham acesso à rede ou simplesmente que sejam executados.

Observa o: Esse recurso só está disponível na instalação do ZENworks Endpoint Security Management e não pode ser usado para políticas de segurança UWS.

Para acessar esse controle, clique na guia *Localizações*, clique no símbolo + ao lado de *Configurações de Firewall*, clique no símbolo + ao lado do firewall desejado e, em seguida, clique no ícone *Controles de Aplicativo* na árvore da política à esquerda.

Para criar uma nova configuração de controle de aplicativo:

1. Na árvore de componentes, clique o botão direito do mouse em *Controles de Aplicativo* e, em seguida, clique em *Adicionar Novos Controles de Aplicativo*.
2. Dê um nome para a lista de controle de aplicativos e forneça uma descrição.
3. Selecione um comportamento de execução. Esse comportamento é usado em todos os aplicativos listados. Se forem necessários vários comportamentos (por exemplo, o acesso à rede é negado a alguns aplicativos de rede, mas a execução é negada a todos os aplicativos de compartilhamento de arquivos), você precisará definir vários controles de aplicativos. Selecione um dos seguintes itens:
   - **Todos Permitidos:** Todos os aplicativos listados têm acesso à rede e permissão para execução.
   - **Nenhuma Execução:** Nenhum aplicativo listado tem permissão para execução.
   - **Sem Acesso à Rede:** Nenhum aplicativo listado tem acesso à rede. O acesso à rede de aplicativos (como browsers da Web) iniciados a partir de um aplicativo também é negado.

   Observa o: Impedir que um aplicativo acesse a rede não afeta a gravação de arquivos em unidades de rede mapeadas. Os usuários podem gravar em todas as unidades de rede disponíveis para eles.
4. Especifique os aplicativos a serem bloqueados. Cada linha deve conter um aplicativo.

Importante: Impedir a execução de aplicativos críticos pode afetar de forma negativa o funcionamento do sistema. Os aplicativos bloqueados do Microsoft Office tentam executar os respectivos programas de instalação.

5 Clique em *Gravar Política*.

Para associar uma lista de controles de aplicativo existentes a essa configuração de firewall:

1 Selecione Controles de Aplicativo na árvore de componentes e clique no botão *Associar Componente*.
2 Selecione uma definição de aplicativo na lista.
3 Configure os aplicativos e o nível de restrição, conforme necessário.

Observa o: Se você mudar as configurações de um componente compartilhado, todas as outras instâncias desse componente serão afetadas. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

4 Clique em *Gravar Política*.

Os controles de aplicativo disponíveis são identificados a seguir. O comportamento de execução padrão é Sem Acesso à Rede.

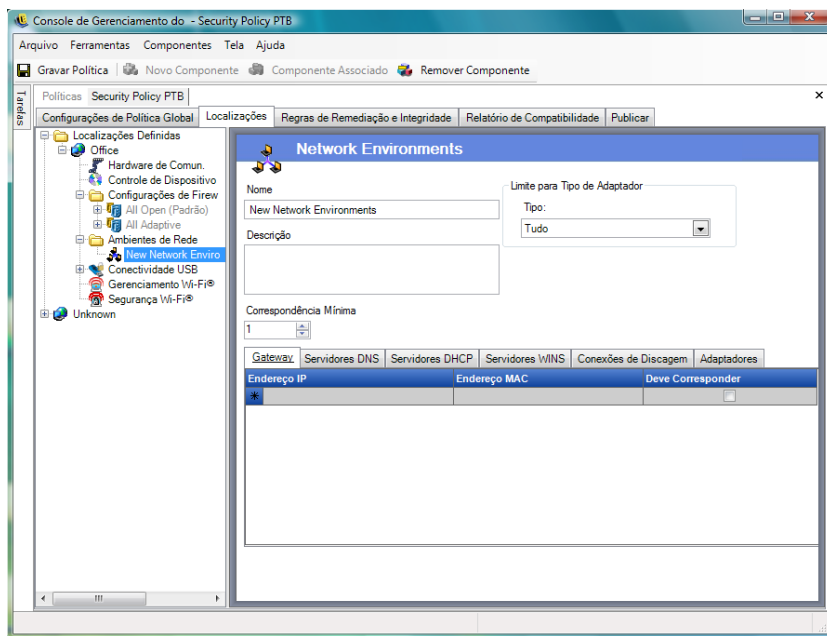
Tabela 2-2 *Controles de Aplicativo*

Nome	Aplicativos
Browsers da Web	explore.exe; netscape.exe; netscp.exe
Mensagens Instantâneas	aim.exe; icq.exe; msmsgs.exe; msnmsgr.exe; trillian.exe; ypager.exe
Compartilhamento de Arquivos	blubster.exe; grokster.exe; imesh.exe; kazaa.exe; morpheus.exe; napster.exe; winmx.exe
Mídia da Internet	mplayer2.exe; wmplayer.exe; naplayer.exe; realplay.exe; spinner.exe; QuickTimePlayer.exe

Se o mesmo aplicativo for adicionado a dois controles de aplicativo diferentes na mesma configuração de firewall (por exemplo, `kazaa.exe` não tem permissão para execução em um controle de aplicativo e não tem permissão para acesso à rede em outro controle de aplicativo com a mesma configuração de firewall), o controle mais estrito do executável específico será aplicado (nesse exemplo, kazaa não será executado).

Ambientes de Rede

Se os parâmetros de rede (servidores Gateway, servidores DNS, servidores DHCP, servidores WINS, pontos de acesso disponíveis ou conexões de adaptadores específicos) forem conhecidos para uma localização, os detalhes do serviço (IP e MAC) que identificam a rede poderão ser inseridos na política para fornecer alternação de localização imediata sem exigir que o usuário grave o ambiente como uma localização.

Para acessar esse controle, clique na guia *Localizações* e, em seguida, clique na pasta *Ambientes de Rede* na árvore da política à esquerda.

As listas permitem que o administrador defina quais serviços de rede estão presentes no ambiente. Cada serviço de rede pode conter diversos endereços. O administrador determina para quantos endereços você precisará encontrar correspondência no ambiente para ativar a alternação de localização.

Use dois ou mais parâmetros de localização em cada definição de ambiente de rede.

Para definir um ambiente de rede:

1. Selecione *Ambientes de Rede* na árvore de componentes e clique no botão *Novo Componente*.
2. Dê um nome para o ambiente de rede e forneça uma descrição.
3. Na lista suspensa *Limitar a Tipo de Adaptador*, determine que tipo de adaptador tem permissão para acessar esse Ambiente de Rede:
   - Sem Fio
   - Todos
   - Modem
   - Com Fio
   - Sem Fio
4. Especifique o número mínimo de serviços de rede necessários para identificar esse ambiente de rede.

   Cada ambiente de rede tem um número mínimo de endereços que o ZENworks Security Client usa para identificá-lo. O número definido em *Correspondência Mínima* não pode exceder o número total de endereços de rede identificados como necessários nas listas com guias. Especifique o número mínimo de serviços de rede necessários para identificar esse ambiente de rede.
5. Especifique as seguintes informações para cada serviço:
   - **Endereço IP:** Especifique até 15 caracteres contendo apenas números de 0 a 9 e pontos. Por exemplo, 123.45.6.789

- **Endereço MAC:** Como alternativa, você pode especificar até 12 caracteres contendo apenas números de 0 a 9 e letras de A a F (maiúsculas e minúsculas), separados por dois-pontos. Por exemplo, 00:01:02:34:05:B6
- Marque a caixa de seleção *Correspondência Certa* se for necessário fornecer a identificação do serviço para definir o ambiente de rede.

6 Nas guias *Conexões por Discagem* e *Adaptadores*, especifique os seguintes requisitos:
   - Em *Conexões por Discagem*, especifique o nome da Entrada RAS da agenda de telefones ou o número discado.

   Observa o: As entradas da agenda de telefones devem conter caracteres alfanuméricos e não podem conter somente caracteres especiais (@, #, $,%, -, etc.) ou caracteres numéricos (1-9). As entradas que só contêm caracteres especiais e numéricos são tratadas como números discados.

   - Em Adaptadores, especifique o SSID de cada adaptador permitido. Os adaptadores devem ser especificados para que seja possível determinar exatamente que adaptadores têm permissão de acesso nesse ambiente de rede. Se nenhum SSID for inserido, todos os adaptadores do tipo permitido terão acesso.

Para associar um ambiente de rede existente a essa localização:

Observa o: A associação de um único ambiente de rede a duas ou mais localizações da mesma política de segurança causa resultados imprevisíveis e não é uma prática recomendável.

---
1 Selecione *Ambientes de Rede* na árvore de componentes e clique no botão *Associar Componente*.

2 Selecione os ambientes de rede na lista.

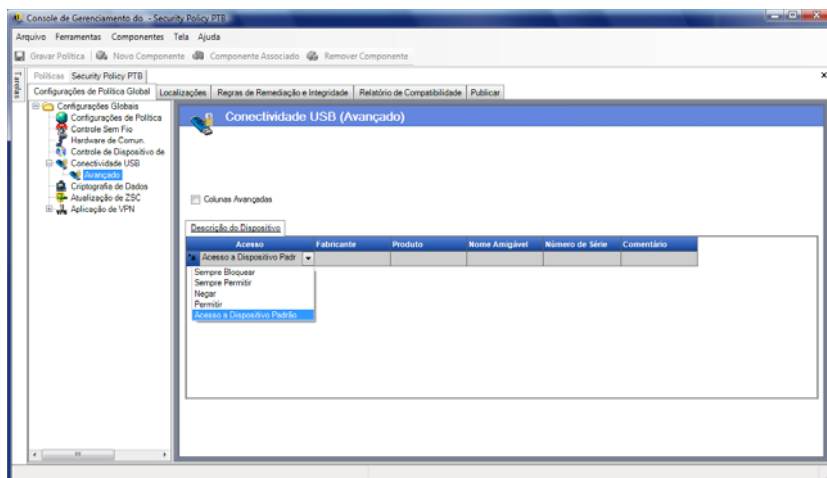
3 Configure os parâmetros de ambiente, conforme necessário.

   Observa o: Se você mudar as configurações de um componente compartilhado, todas as outras instâncias desse componente serão afetadas. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

   ---
4 Clique em *Gravar Política*.

Conectividade USB

Todos os dispositivos que se conectam por meio do barramento USB podem ser permitidos ou negados pela política. Esses dispositivos podem ser explorados na política a partir do relatório Inventário de Dispositivos USB. Também é possível que todos os dispositivos conectados à máquina no momento sejam explorados simultaneamente. Esses dispositivos podem ser filtrados por fabricante, nome do produto, número de série, tipo, etc. Para fins de suporte, o administrador pode configurar a política para aceitar um conjunto de dispositivos por tipo de fabricante (por exemplo, todos os dispositivos HP são permitidos) ou por tipo de produto (por exemplo, todos os dispositivos USB de interface com o usuário, como mouse e teclado, são permitidos). Além disso, dispositivos individuais podem ser permitidos para impedir que dispositivos sem suporte sejam inseridos na rede (por exemplo, nenhuma impressora é permitida, exceto a impressora da política).

Para acessar esse controle, clique na guia *Configurações de Política Global* e, em seguida, clique em *Conectividade USB* na árvore de política à esquerda.

Especifique que o acesso a qualquer dispositivo que não esteja na lista deve ser permitido ou negado.

Os seguintes métodos permitem que você preencha a lista a fim de permitir ou negar conectividade USB aos dispositivos:

- "Adicionando dispositivos manualmente" na página 89
- "Importando listas de dispositivos" na página 89

Adicionando dispositivos manualmente

1. Insira o dispositivo na porta USB da máquina em que o Console de Gerenciamento está instalado.
2. Quando o dispositivo estiver pronto, clique no botão *Explorar*. Se o dispositivo tiver um número de série, sua descrição e seu número de série serão exibidos na lista.
3. Selecione uma configuração na lista suspensa (a configuração *Dispositivo Removível Global* não se aplica a essa política):
   - **Habilitar:** Os dispositivos da lista de preferidos recebem autorização total para leitura/ gravação; todos os outros dispositivos USB e de armazenamento externos são desabilitados.
   - **Apenas Leitura:** Os dispositivos da lista de preferidos recebem autorização apenas leitura; todos os outros dispositivos USB e de armazenamento externos são desabilitados.

Repita essa etapas para cada dispositivo permitido na política. A mesma configuração será aplicada a todos os dispositivos.

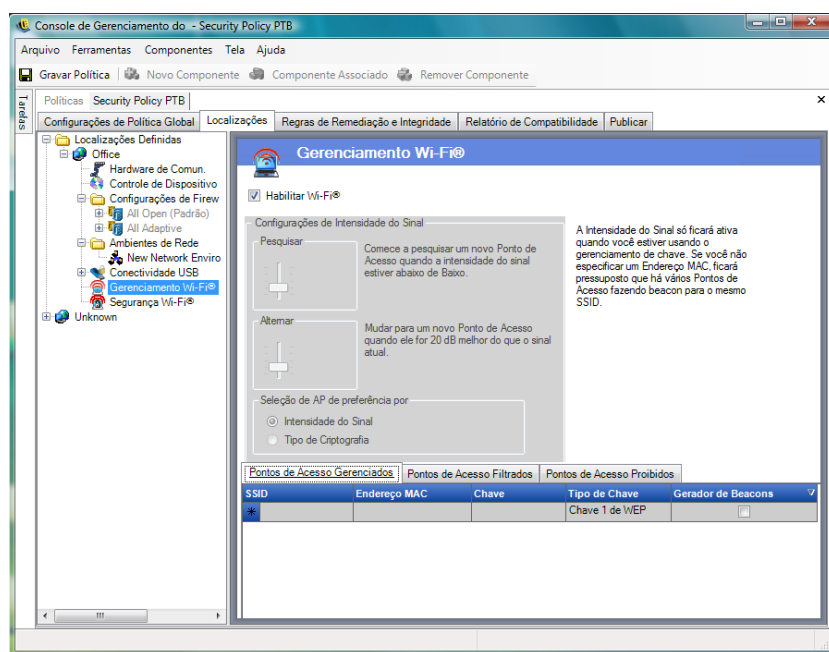
Importando listas de dispositivos

O aplicativo Scanner da Unidade USB da Novell gera uma lista de dispositivos e dos respectivos números de série (Seção 1.11, "Scanner da Unidade USB" na página 42). Para importar essa lista, clique em *Importar* e navegue até ela. A lista preenche os campos *Descrição* e *Número de Série*.

Gerenciamento de Wi-Fi

O gerenciamento de Wi-Fi permite que o administrador crie listas de Pontos de Acesso. Os pontos de acesso sem fio inseridos nessas listas determinam a quais pontos de acesso o ponto de extremidade pode se conectar na localização e quais pontos de acesso o ponto de extremidade pode ver no Gerenciador de Configuração Zero (Configuração Zero) da Microsoft. Gerenciadores de configuração sem fio de terceiros não são suportados com essa funcionalidade. Se nenhum ponto de acesso for inserido, todos estarão disponíveis para o ponto de extremidade.

Para acessar esse controle, clique na guia *Localizações* e, em seguida, clique em *Gerenciamento de Wi-Fi* na árvore da política à esquerda.

Observa o: Em Segurança Wi-Fi ou Gerenciamento de Wi-Fi, se você desmarcar a opção *Habilitar*, toda a conectividade Wi-Fi da localização será desabilitada.

Se você inserir pontos de acesso na lista *Pontos de Acesso Gerenciados*, a Configuração Zero será desativada e o ponto de extremidade será forçado a só se conectar aos pontos de acesso listados quando eles estiverem disponíveis. Se os pontos de acesso gerenciados não estiverem disponíveis, o ZENworks Security Client volta para a Lista de Pontos de Acesso Filtrados. Os pontos de acesso inseridos em Pontos de Acesso Proibidos nunca são exibidos na Configuração Zero.

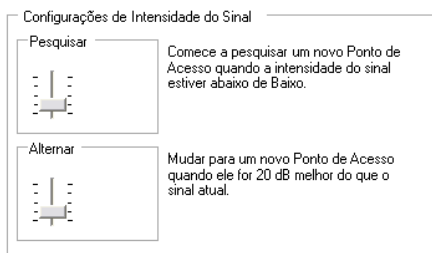
Observa o: A lista de pontos de acesso só é suportada no sistema operacional Windows* XP. Antes de distribuir uma lista de pontos de acesso, é recomendável que todos os pontos de extremidade limpem a lista de redes preferenciais da Configuração Zero.

As seções a seguir contêm mais informações:

- "Configurações de Força do Sinal Wi-Fi" na página 91
- "Pontos de Acesso Gerenciados" na página 92

* “Pontos de Acesso Filtrados” na página 93
* “Pontos de Acesso Proibidos” na página 93

Configurações de Força do Sinal Wi-Fi

Quando mais de um ponto de acesso gerenciado por WEP é definido na lista, é possível estabelecer a força do sinal necessária para alternar para o adaptador Wi-Fi. Os limites de força do sinal podem ser ajustados por localização para que seja possível determinar quando o ZENworks Security Client deve procurar, descartar e alternar para outro ponto de acesso definido na lista.

É possível ajustar as seguintes informações:

* **Pesquisar:** Quando esse nível de força de sinal é alcançado, o ZENworks Security Client começa a pesquisar um novo ponto de acesso ao qual se conectar. A configuração padrão é Baixo [-70 dB].
* **Alternar:** Para que o ZENworks Security Client se conecte a um novo ponto de acesso, esse ponto de acesso deve transmitir no nível de força de sinal designado acima da conexão atual. A configuração padrão é de +20 dB.

Os limites de força do sinal são determinados pela quantidade de força (em dB) reportada por meio do driver de miniporta do computador. Como cada placa ou rádio Wi-Fi pode tratar os sinais dB de maneira diferente para o RSSI (Received Signal Strength Indication), os números variam de adaptador para adaptador.

Você pode definir sua preferência para a seleção de ponto de acesso com base no seguinte:

* Força do Sinal
* Tipo de Criptografia

Os números padrão associados aos limites definidos no Console de Gerenciamento são genéricos para a maioria dos adaptadores Wi-Fi. Você deve pesquisar os valores RSSI do seu adaptador Wi-Fi para inserir um nível preciso. Os valores da Novell são:

Nome	Valor Padrão
Excelente	-40 dB
Muito Bom	-50 dB
Bom	-60 dB
Baixo	-70 dB
Muito Baixo	-80 dB

Observa o: Embora os nomes de força de sinal acima correspondam aos usados pelo Serviço de Configuração Zero da Microsoft, os limites podem não ser correspondentes. A Configuração Zero determina seus valores com base no SNR (Signal to Noise Ratio) e não somente no valor de dB reportado do RSSI. Por exemplo, se um adaptador Wi-Fi estiver recebendo um sinal a -54 dB e tiver um nível de ruído de -22 dB, o SNR reportará 32dB (-54 - -22=32), o que na escala de Configuração Zero representa uma força de sinal Excelente. No entanto, na escala da Novell, o sinal -54 dB (se reportado dessa maneira pelo driver de miniporta) indica um sinal Muito Bom.

É importante notar que o usuário final nunca vê os limites de força de sinal da Novell; essa informação é fornecida para mostrar a diferença entre o que o usuário pode ver na Configuração Zero e o que realmente ocorre.

Pontos de Acesso Gerenciados

O ZENworks Endpoint Security Management fornece um processo simples para distribuir e aplicar automaticamente chaves do protocolo WEP (Wired Equivalent Privacy) sem a intervenção do usuário (ignorando e encerrando o gerenciador de Configuração Zero da Microsoft). Isso protege a integridade das chaves, pois elas não são passadas em e-mails ou memorandos escritos sem criptografia. Na verdade, o usuário final nunca precisa conhecer a chave para se conectar automaticamente ao ponto de acesso. Isso ajuda a evitar a possível redistribuição das chaves para usuários não autorizados.

Devido às vulnerabilidades de segurança inerentes à Autenticação de Chave WEP, a Novell só suporta a autenticação de Chave WEP Aberta. Com a autenticação compartilhada, o processo de validação de chave AP/cliente envia uma versão sem criptografia e uma versão com criptografia de uma frase de verificação que é facilmente detectada no modo sem fio. Isso pode dar a um hacker as versões com e sem criptografia da frase. Quando obtiver essa informação, ele conseguirá decifrar a chave facilmente.

Forneça as seguintes informações para cada ponto de acesso:

- **SSID:** Identifique o número SSID. O número SSID faz diferenciação entre maiúsculas e minúsculas.
- **Endereço MAC:** Identifique o endereço MAC (é recomendável devido à semelhança entre SSIDs). Se o endereço não for especificado, o sistema pensará que há vários pontos de acesso transmitindo beacon do mesmo número SSID.
- **Chave:** Especifique a chave WEP do ponto de acesso (10 ou 26 caracteres hexadecimais).
- **Tipo de Chave:** Identifique o índice de chave criptográfica selecionando o nível apropriado na lista suspensa.
- **Beaconing:** Verifique se o ponto de acesso definido está transmitindo seu SSID. Mantenha essa opção desmarcada se for um ponto de acesso sem beaconing.

Observa o: O ZENworks Security Client tenta estabelecer conexão com cada ponto de acesso de beaconing listado na política. Se nenhum acesso de beaconing for localizado, o ZENworks Security Client tentará estabelecer conexão com qualquer ponto de acesso sem beaconing (identificado por SSID) listado na política.

Quando um ou mais pontos de acesso são definidos na lista *Pontos de Acesso Gerenciados*, a alternância da Força do Sinal do adaptador Wi-Fi também pode ser definida.

Pontos de Acesso Filtrados

Os pontos de acesso inseridos na lista *Pontos de Acesso Filtrados* são os únicos pontos de acesso exibidos na Configuração Zero. Isso impede que o ponto de extremidade se conecte a pontos de acesso não autorizados.

Forneça as seguintes informações para cada ponto de acesso:

- **SSID:** Identifique o número SSID. O número SSID faz diferenciação entre maiúsculas e minúsculas.
- **Endereço MAC:** Identifique o endereço MAC (é recomendável devido à semelhança entre SSIDs). Se o endereço não for especificado, o sistema pensará que há vários pontos de acesso transmitindo beacon do mesmo SSID.

Pontos de Acesso Proibidos

Os pontos de acesso inseridos na lista Pontos de Acesso Proibidos não serão exibidos no Zero Config e o ponto de acesso não poderá se conectar a eles.

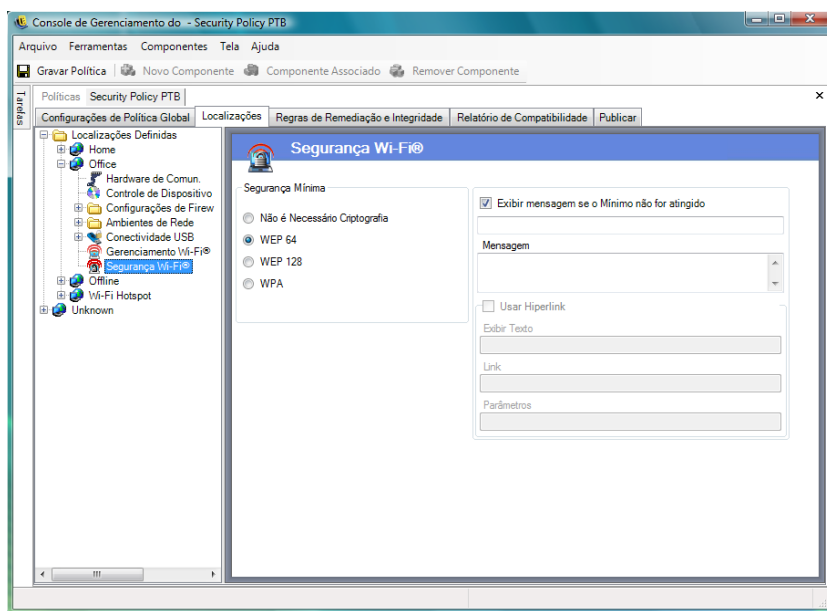
Forneça as seguintes informações para cada ponto de acesso:

- **SSID:** Identifique o número SSID. O número SSID faz diferenciação entre maiúsculas e minúsculas.
- **Endereço MAC:** Identifique o endereço MAC (recomendado devido à semelhança entre SSIDs). Se o endereço não for especificado, o sistema pensará que há vários pontos de acesso transmitindo beacon do mesmo SSID.

Segurança Wi-Fi

Se o Hardware de Comunicação Wi-Fi (placas PCMCIA ou de outro tipo para adaptadores Wi-Fi e rádios Wi-Fi integrados) for permitido globalmente (consulte "Controle Sem Fio" na página 50), será possível aplicar configurações adicionais ao adaptador nessa localização.

Para acessar esse controle, clique na guia *Localizações* e, em seguida, clique em *Segurança Wi-Fi* na árvore da política à esquerda.

Observa o: Em Segurança Wi-Fi ou Gerenciamento de Wi-Fi, se você desmarcar a opção *Habilitar*, toda a conectividade Wi-Fi da localização será desabilitada.

O adaptador Wi-Fi pode ser configurado para se comunicar somente com pontos de acesso com um nível específico de criptografia em um determinado local.

Por exemplo, se uma configuração de WPA de pontos de acesso for distribuída em uma filial, o adaptador poderá ficar restrito a comunicações com pontos de acesso com nível de criptografia WEP de 128 bits ou maior. Isso impede que o adaptador se associe acidentalmente a pontos de acesso suspeitos e não seguros.

Uma mensagem personalizada para o usuário deve ser escrita quando a configuração for colocada acima de *Nenhuma Criptografia Necessária*.

Você pode definir uma preferência para a conexão com pontos de acesso por ordem do nível de criptografia ou pela força do sinal quando dois ou mais pontos de acesso são inseridos nas listas *Pontos de Acesso Gerenciados* e *Pontos de Acesso Filtrados*. O nível selecionado impõe a conectividade com pontos de acesso que atendam ao requisito de criptografia mínimo ou superior.

Por exemplo, se WEP 64 for o requisito de criptografia e se a criptografia for a preferência, os pontos de acesso com a maior força de criptografia terão prioridade sobre todos os outros. Se a força do sinal for a preferência, o sinal mais forte terá prioridade no momento da conexão.

2.2.3 Regras de Integridade e Correção

O ZENworks Endpoint Security Management permite verificar se o software necessário está sendo executado no ponto de extremidade e fornece procedimentos de correção imediatos caso ocorra falha na verificação.

As seções a seguir contêm mais informações:

- "Regras de spyware e antivírus" na página 95
- "Testes de integridade" na página 96
- "Verificações de integridade" na página 98
- "Regras de Script Avançadas" na página 99

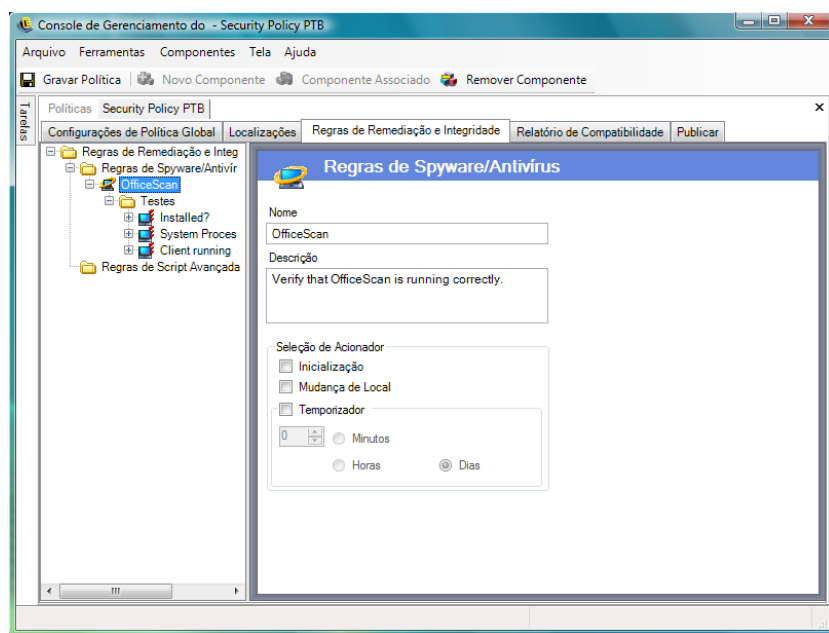
Regras de spyware e antivírus

As regras de spyware e antivírus verificam se os softwares antivírus ou spyware designados no ponto de extremidade estão em execução e atualizados. São realizados testes para determinar se o software está em execução e se a versão está atualizada. Se ambas as verificações forem bem-sucedidas, será permitido alternar para qualquer localização definida. A falha em um dos testes poderá resultar nas seguintes ações (definidas pelo administrador):

- Um relatório é enviado ao Serviço de Geração de Relatórios.
- Uma mensagem personalizada para o usuário é exibida, com um link de inicialização opcional contendo informações sobre como corrigir a violação da regra.
- O usuário passa para o estado de quarentena, o que limita seu acesso à rede e proíbe que determinados programas acessem a rede. Essas medidas impedem que o usuário infecte ainda mais a rede.

Depois que um teste de acompanhamento comprova a conformidade dos pontos de extremidade, as configurações de segurança recuperam automaticamente seu estado original.

Observa o: Esse recurso só está disponível na instalação do ZENworks Endpoint Security Management e não pode ser usado para políticas de segurança UWS.

Para acessar esse controle, clique na guia *Regras de Remediação e Integridade* e, em seguida, clique em *Regras de Spyware/Antivírus* na árvore de políticas à esquerda.

Poderão ser criados testes personalizados para softwares que não estejam na lista padrão. Um único teste pode ser criado para executar verificações em um ou mais softwares de acordo com a mesma regra. Cada conjunto de verificações Processo em Execução e Arquivo Existente terá seus próprios resultados de êxito e falha.

Para criar uma nova regra de spyware ou antivírus:

1. Na árvore de componentes, selecione *Regras de Spyware/Antivírus* e clique em *Novo Spyware/ Antivírus*.
2. Clique em *Novo Componente*.
3. Dê um nome para a regra e forneça uma descrição.
4. Selecione o acionador da regra:
   - **Inicialização:** Executar testes na inicialização do sistema.
   - **Mudança de Localização:** Executar testes sempre que o ZENworks Security Client mudar para outra localização.
   - **Temporizador:** Executar testes de integridade em uma programação definida por minuto, hora ou dia.
5. Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, "Notificação de erros" na página 106.
6. Defina os testes de integridade.

Para associar regras de spyware ou antivírus existentes:

1. Selecione *Regras de Spyware/Antivírus* e clique em *Associar Componente*.
2. Selecione as regras desejadas na lista.
3. (Opcional) Redefina os testes, as verificações e os resultados.

   Observa o: Se você mudar as configurações de um componente compartilhado, todas as outras instâncias desse componente serão afetadas. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

   ---

4. Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, "Notificação de erros" na página 106.

As verificações e os testes de integridade são incluídos automaticamente e, se necessário, podem ser editados.

Testes de integridade

Cada teste de integridade pode executar duas verificações: *Arquivo Existente* e *Processo em Execução*. Cada teste tem seus próprios resultados de êxito e falha.

Há testes padrão e verificações pré-escritas para todas as regras de spyware e antivírus definidas. É possível incluir testes adicionais na regra de integridade.

Se houver vários testes, eles serão executados na ordem inserida aqui. É necessário que o primeiro teste seja concluído com êxito para que o teste seguinte seja executado.

Para criar um teste de integridade:

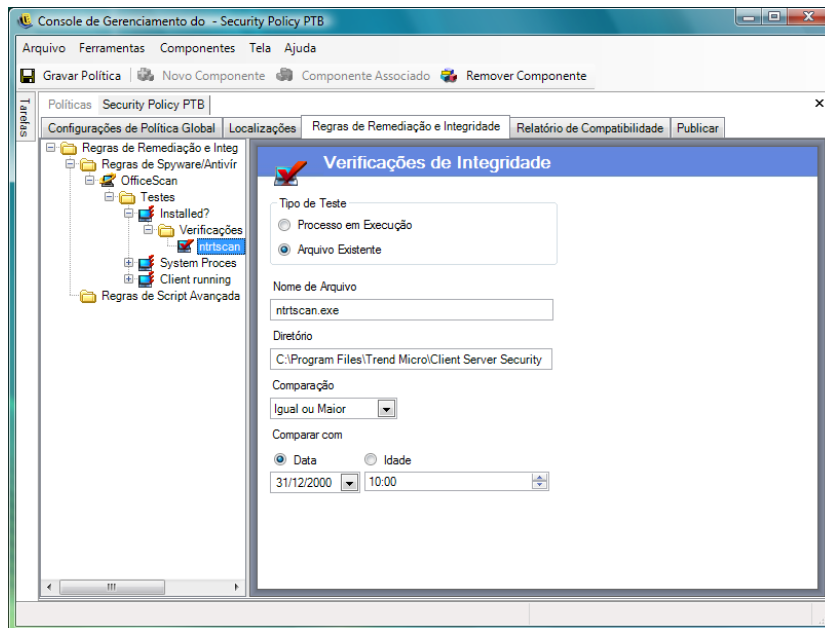
1. Na árvore de componentes, selecione *Testes de Integridade*, clique no sinal de + ao lado do relatório desejado para expandir a lista, clique o botão direito do mouse em *Testes* e, em seguida, clique em *Adicionar Novos Testes*.
2. Dê um nome para o teste e forneça uma descrição.
3. Especifique o texto do relatório de êxito do teste.
4. Defina o seguinte para o caso de ocorrer falha no teste:
   - **Continuar após Falha:** Selecione essa opção para que o usuário possa continuar com a conectividade de rede mesmo que o teste falhe ou para que o teste seja repetido.
   - **Firewall:** Essa configuração será aplicada em caso de falha no teste. As configurações Todos Fechados, Integridade Não Compatível ou um firewall de quarentena personalizado impedem que o usuário se conecte à rede.
   - **Mensagem:** Selecione a mensagem personalizada para o usuário a ser exibida em caso de falha no teste. Essa mensagem pode incluir etapas de correção para o usuário final.
   - **Relatório:** Forneça o relatório de falhas enviado para o serviço de geração de relatórios.
5. Forneça uma mensagem de falha. Essa mensagem só é exibida quando ocorrem falhas em uma ou mais verificações. Clique na caixa de seleção e especifique as informações da mensagem nas caixas fornecidas.
6. É possível adicionar um hiperlink para fornecer opções de correção. Pode ser um link para informações adicionais ou um link para download de patches ou atualizações relacionados à falha do teste (consulte Seção , “Hiperlinks” na página 68).

7 Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, “Notificação de erros” na página 106.

8 Defina as verificações de integridade.

9 Se desejar, repita as etapas descritas acima para criar um novo teste de spyware ou antivírus.

Verificações de integridade

As verificações de cada teste determinam se um ou mais processos de spyware/antivírus estão sendo executados ou se existem arquivos essenciais. É preciso definir pelo menos uma verificação para que um teste de integridade seja executado.

Para criar uma nova verificação, clique o botão direito do mouse em *Verificações de Integridade* na árvore da política à esquerda e, em seguida, clique em *Adicionar Novas Verificações de Integridade*. Selecione um dos dois tipos de verificação e forneça as informações descritas a seguir:

Processo em Execução: Determine se o software está sendo executado no momento do evento acionador (por exemplo, o cliente AV). A única informação necessária para essa verificação é o nome do executável.

Arquivo Existente: Use essa verificação para determinar se o software está atualizado no momento do evento acionador.

Insira as seguintes informações nos campos fornecidos:

- **Nome do Arquivo:** Especifique o nome de arquivo a ser verificado.
- **Diretório do Arquivo:** Especifique o diretório em que o arquivo reside.
- **Comparação do Arquivo:** Selecione uma comparação de datas na lista suspensa:
    - Nenhum
    - Igual

- Igual ou Maior
- Igual ou Menor

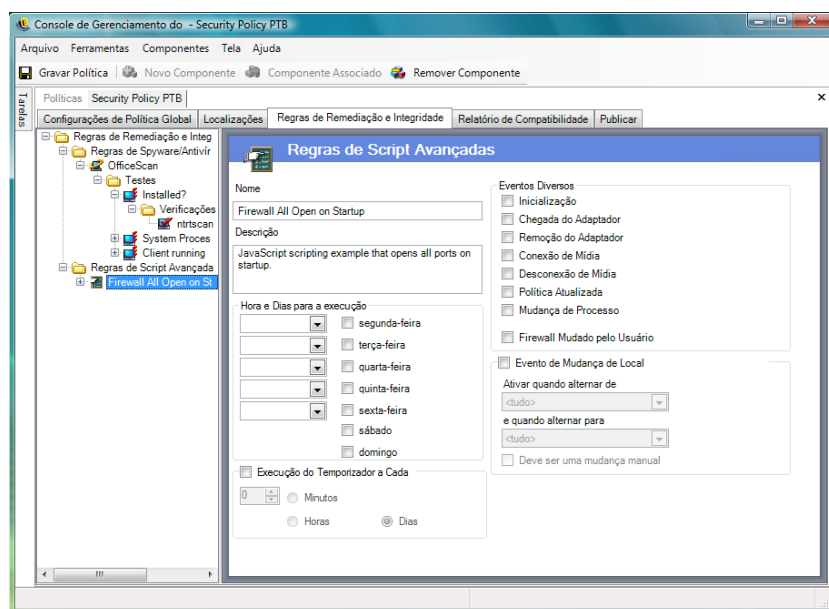
- **Comparar por:** Especifique *Duração* ou *Data*.
  - *Data* garante que o arquivo não seja mais antigo do que a data e a hora especificadas (por exemplo, a data da última atualização).
  - *Duração* garante que o arquivo não seja mais antigo do que um período especificado, medido em dias.

Observa o: A comparação de arquivos Igual é tratada como Igual ou Menor quando a verificação *Duração* é usada.

As referências são executadas na ordem em que são inseridas.

Regras de Script Avançadas

O ZENworks Endpoint Security Management inclui uma ferramenta avançada de criação de scripts de regras que permite aos administradores criar regras extremamente flexíveis e complexas e ações de correção.

Para acessar esse controle, clique em *Regras de Remediação e Integridade* e, em seguida, clique no ícone *Regras de Script Avançadas* na árvore da política à esquerda.

A ferramenta de criação de scripts usa uma das linguagens comuns de criação de scripts, VBScript ou JScript, para criar regras que contenham um acionador (quando executar a regra) e o script real (a lógica da regra). O administrador não está limitado ao tipo de script executado.

A criação de scripts avançada é implementada de forma seqüencial, juntamente com outras regras de integridade. Portanto, um script de longa execução só permitirá que outras regras (inclusive regras programadas) sejam executadas depois de ser concluído.

Para criar uma nova regra de script avançada:

1. Na árvore de componentes, clique o botão direito do mouse em *Regras de Script Avançadas* e, em seguida, clique em *Adicionar Novas Regras de Script*.
2. Dê um nome para a regra e forneça uma descrição.
3. Especifique os eventos acionadores.
   - **Horários e Dias de Execução:** Especifique cinco horários diferentes para a execução do script. O script é executado semanalmente, nos dias selecionados.
   - **Temporizador Executado a Cada:** Especifique a freqüência de execução do temporizador.
   - **Eventos Diversos:** Especifique os eventos no ponto de extremidade que aciona o script.
   - **Evento de Mudança de Localização:** Especifique o evento de mudança de localização que aciona o script. Esses eventos não são independentes; eles são complementares ao evento anterior.
     - **Verificar Evento de Localização:** O script é executado em todas as mudanças de localização.
     - **Ativar quando alternar de:** O script é executado apenas quando o usuário sai dessa localização (especificada) e vai para outra.
     - **Ativar quando alternar para:** O script é executado quando o usuário sai de qualquer outra localização e entra na localização especificada. Se o campo *Ativar quando alternar de* for preenchido com um parâmetro de localização (por exemplo, Escritório), o script só será executado quando a localização alternar de Escritório para a localização especificada.
     - **Deve ser mudança manual:** O script só é executado quando o usuário alterna manualmente de ou para uma localização.
4. Crie variáveis de script. Para obter mais informações, consulte "Variáveis de script" na página 101.
5. Escreva o texto do script. Para obter mais informações, consulte "Texto do Script" na página 102.
6. Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, "Notificação de erros" na página 106.

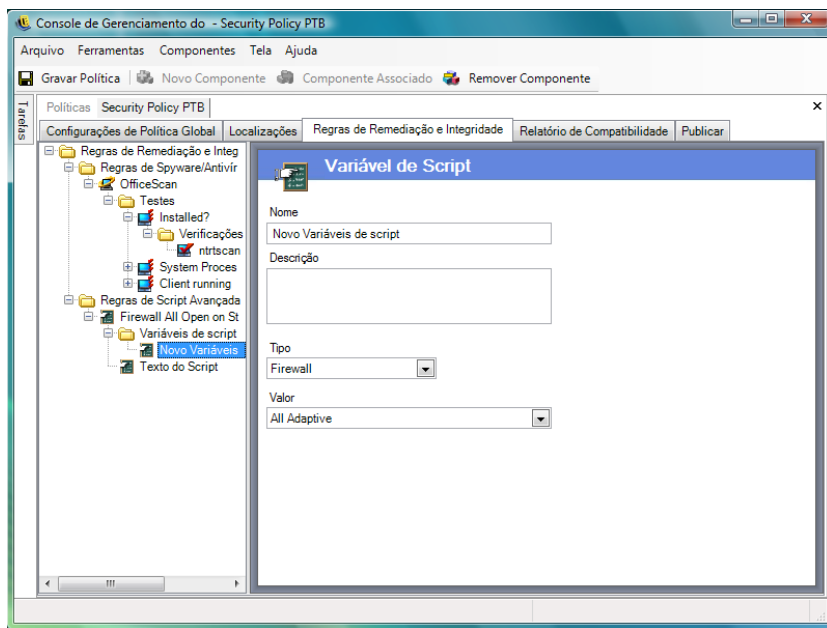
Para associar uma regra de script avançada existente:

1. Na árvore de componentes, selecione *Regras de Script Avançadas* e clique em *Associar Novo*.
2. Selecione as regras desejadas na lista.
3. Se necessário, redefina o evento acionador, as variáveis ou o script.

   Observa o: Se você mudar as configurações de um componente compartilhado, todas as outras instâncias desse componente serão afetadas. Use o comando *Mostrar Uso* para ver todas as outras políticas associadas ao componente.

4. Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, "Notificação de erros" na página 106.

Variáveis de script

Essa é uma configuração opcional que permite ao administrador definir uma variável (var) para o script, além de possibilitar que ele opte por usar a funcionalidade ZENworks Endpoint Security Management (por exemplo, iniciar mensagens personalizadas para o usuário e hiperlinks definidos; alternar para uma localização ou uma configuração de firewall definida) ou mudar o valor de uma variável sem mudar o script propriamente dito.

Para criar uma nova variável de script:

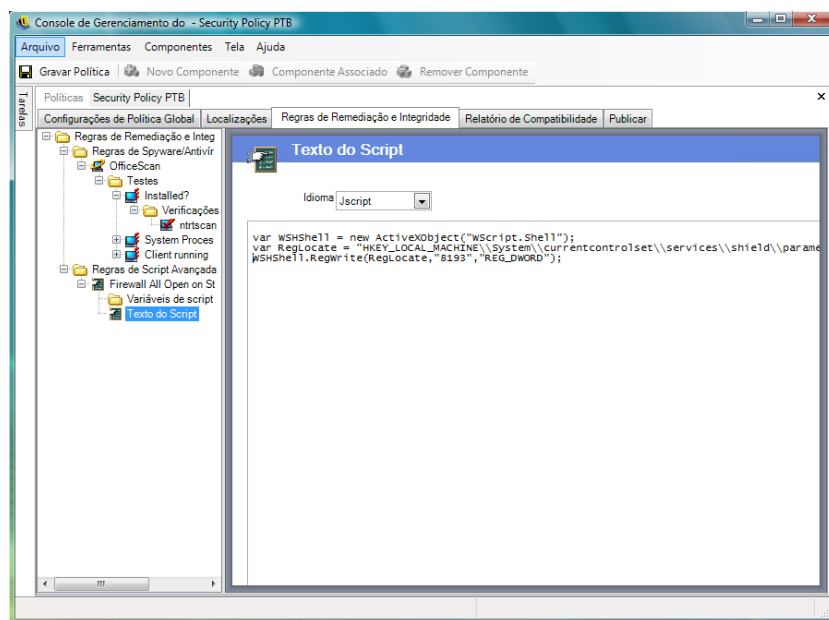
1. Na árvore de componentes, clique o botão direito do mouse em *Variáveis de Script* e, em seguida, clique em *Adicionar Novas Variáveis*.
2. Dê um nome para a variável e forneça uma descrição.
3. Selecione o tipo de variável:
    - **Mensagens Personalizadas para o Usuário:** Define uma mensagem personalizada para o usuário que pode ser iniciada como ação.
    - **Firewall:** Define uma configuração de firewall que pode ser aplicada como ação.
    - **Hiperlinks:** Define um hiperlink que pode ser iniciado como ação.
    - **Localização:** Define uma localização que pode ser aplicada como ação.
    - **Número:** Define um valor numérico.
    - **String:** Define um valor de string.
4. Especifique o valor da variável:
    - Tudo Adaptável
    - Tudo Fechado
    - Tudo Aberto

- Novas Configurações de Firewall
- Integridade Incompatível

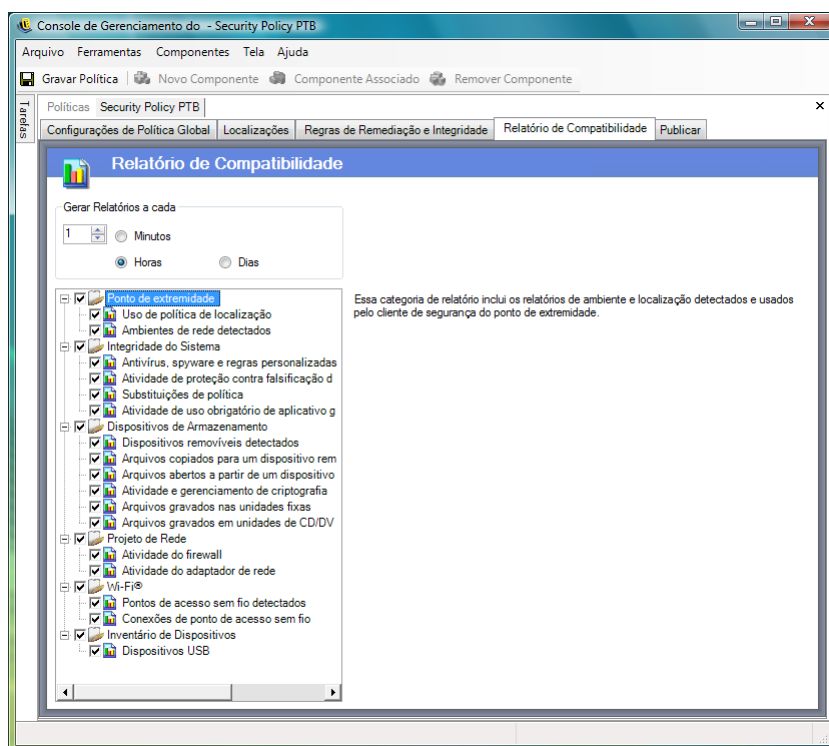
5 Clique em *Gravar Política*. Se houver erros na política, consulte Seção 2.2.6, “Notificação de erros” na página 106.

Texto do Script

O administrador o ZENworks Endpoint Security Management não é limitado ao tipo de script que pode ser executado pelo ZENworks Security Client. Todos os scripts devem ser testados antes da distribuição da política.

Selecione o tipo de script (Jscript ou VBscript) e insira o texto do script no campo. É possível copiar o script de outra origem e colá-lo no campo.

2.2.4 Gerador de Relatórios de Compatibilidade

Devido ao nível e ao acesso dos drivers do ZENworks Security Client, praticamente todas as transações executadas pelo ponto de extremidade podem ser reportadas. O ponto de extremidade pode executar cada inventário de sistemas opcionais para fins de solução de problemas e criação de políticas. Para acessar esses relatórios, clique na guia *Relatório de Compatibilidade*.

Observa o: O gerador de relatórios não está disponível quando o Console de Gerenciamento Independente está sendo executado.

Para executar o gerador de relatórios de conformidade para essa política:

1. Especifique a freqüência de geração de relatórios. Isso representa a freqüência com que os dados serão carregados do ZENworks Security Client para o Serviço de Distribuição de Políticas.
2. Verifique cada categoria, ou tipo, de relatório a ser capturado.

Os seguintes relatórios estão disponíveis:

Ponto de Extremidade

- **Uso de política de localização:** O ZENworks Security Client reporta todas as políticas de localização obrigatórias e a duração desse uso obrigatório.
- **Ambientes de rede detectados:** O ZENworks Security Client reporta todas as configurações de ambiente de rede detectadas.

Integridade do Sistema

- **Antivírus, spyware e regras personalizadas:** O ZENworks Security Client reporta as mensagens de integridade configuradas com base nos resultados do teste.
- **Atividade de proteção contra falsificação de ponto de extremidade:** O ZENworks Security Client reporta qualquer tentativa de violação do cliente de segurança.
- **Substituições de política:** O ZENworks Security Client reporta qualquer tentativa de substituição administrativa no cliente de segurança.
- **Atividade para assegurar o uso obrigatório de aplicativo gerenciado:** O ZENworks Security Client reporta qualquer atividade de uso obrigatório de aplicativos gerenciados.

Dispositivos de Armazenamento

- **Dispositivos removíveis detectados:** O ZENworks Security Client reporta todos os dispositivos de armazenamento removíveis detectados pelo cliente de segurança.
- **Arquivos copiados para um dispositivo removível:** O ZENworks Security Client reporta arquivos copiados em um dispositivo de armazenamento removível.
- **Arquivos abertos a partir de um dispositivo removível:** O ZENworks Security Client reporta arquivos abertos em um dispositivo de armazenamento removível.
- **Atividade e gerenciamento de criptografia:** O ZENworks Security Client reporta atividade de criptografia/decodificação usando a Solução de Criptografia de Armazenamento do ZENworks.
- **Arquivos gravados em unidades fixas:** O ZENworks Security Client reporta o número de arquivos gravados nas unidades fixas do sistema.
- **Arquivos gravados nas unidades de CD/DVD:** O ZENworks Security Client reporta o número de arquivos gravados nas unidades de CD/DVD do sistema.

Projeto de Rede

- **Atividade do firewall:** O ZENworks Security Client reporta todo tráfego bloqueado pelo firewall configurado para a política de localização aplicada.

  Importante: A habilitação desse relatório pode resultar em grandes volumes de dados. Os dados podem saturar um banco de dados rapidamente. O teste de um ZENworks Security Client reportou 1.115 uploads de dados de pacotes bloqueados durante um período de 20 horas. Antes de realizar uma distribuição em larga escala, você deve executar um período de monitoramento e ajuste com um cliente de teste no ambiente afetado.

- **Atividade do adaptador de rede:** O ZENworks Security Client reporta todo o tráfego de um dispositivo de rede gerenciado.

Wi-Fi

- **Pontos de acesso sem fio detectados:** O ZENworks Security Client reporta todos os pontos de acesso detectados.
- **Conexões de ponto de acesso sem fio:** O ZENworks Security Client reporta todas as conexões de ponto de acesso estabelecidas pelo ponto de extremidade.

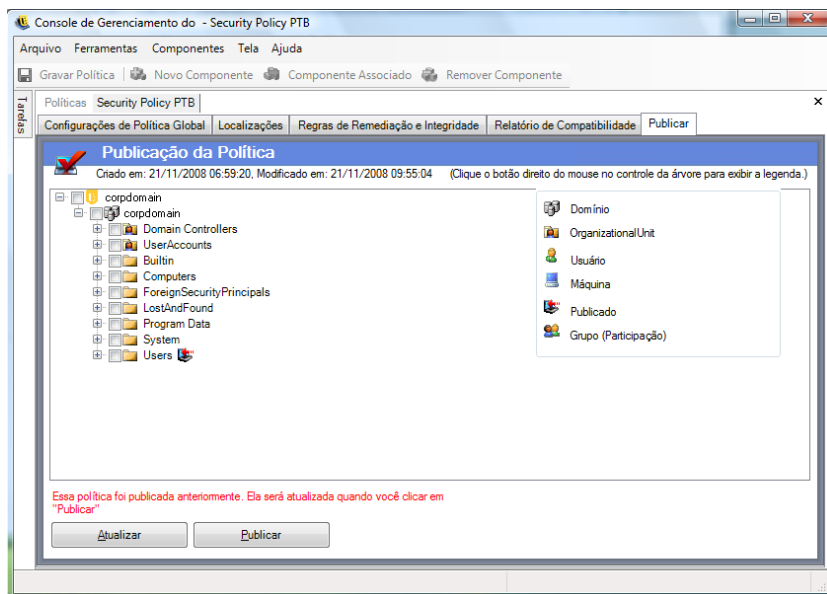
Inventário de Dispositivos

- **Dispositivos USB:** O ZENworks Security Client reporta todos os dispositivos USB detectados no sistema.

2.2.5 Publicar

Políticas de segurança concluídas são enviadas aos usuários pelo mecanismo de publicação. Depois de publicada, a política pode ser atualizada quando os usuários recebem atualizações em entradas programadas. Para publicar uma política, clique na guia *Publicar*. As seguintes informações são exibidas:

- A árvore de diretórios atual

- As datas de criação e modificação da política
- Os botões *Atualizar* e *Publicar*

Com base nas permissões de publicação atuais do usuário, a árvore de diretórios pode ser exibida com uma ou mais seleções em vermelho. Os usuários não têm permissão para enviar publicações para usuários/grupos exibidos em vermelho.

Os usuários e os grupos associados a eles só são exibidos após a autenticação no Serviço de Gerenciamento. As mudanças no serviço de diretório corporativo podem não ser exibidas imediatamente no Console de Gerenciamento. Clique em *Atualizar* para atualizar a árvore de diretórios do Serviço de Gerenciamento.

As seções a seguir contêm mais informações:

- "Publicando uma política" na página 105
- "Atualizando uma política publicada" na página 106

Publicando uma política

1. Selecione um grupo de usuários (ou um usuário individual) na árvore de diretórios à esquerda. Clique duas vezes nos usuários para selecioná-los (se um grupo de usuários for selecionado, todos os usuários serão incluídos).

   O ícone aparecerá ao lado dos nomes dos usuários que não receberam a política. O ícone aparecerá ao lado dos nomes dos usuários ou dos grupos que já receberam a política.

   Para anular a seleção de um usuário ou de um grupo, clique duas vezes no usuário ou no grupo para remover o ícone .

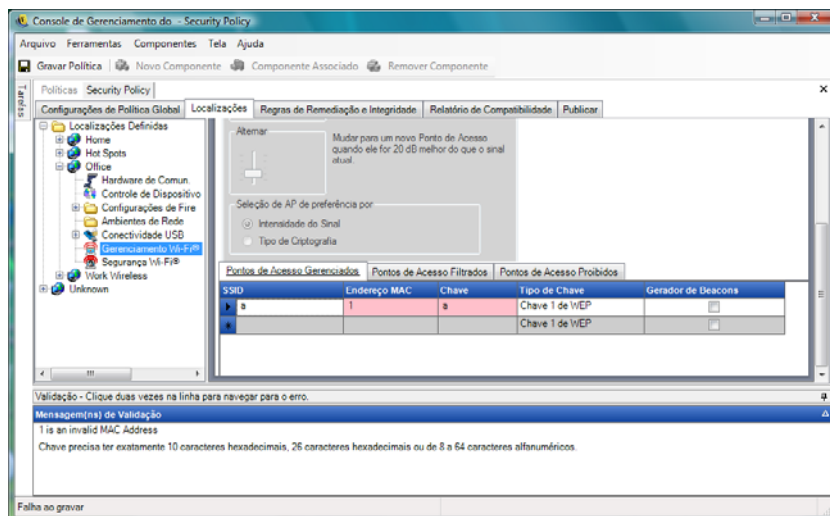
2. Clique em *Publicar* para enviar a política ao Serviço de Distribuição de Políticas.

Atualizando uma política publicada

Após uma política ser publicada para os usuários, atualizações simples poderão ser mantidas por meio da edição dos componentes e da republicação da política. Por exemplo, se o administrador do ZENworks Endpoint Security Management precisar mudar a chave WEP de um ponto de acesso, ele só precisará editar a chave, gravar a política e clicar em *Publicar*. Os usuários afetados receberão a política atualizada (e a nova chave) em sua próxima entrada.

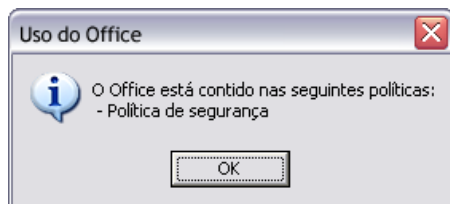
2.2.6 Notificação de erros

Quando o administrador tenta gravar uma política com dados incompletos ou incorretos em um componente, o painel Validação é exibido na parte inferior do Console de Gerenciamento, destacando cada erro. Os erros devem ser corrigidos para que a política possa ser gravada.

Clique duas vezes em cada linha da validação para navegar até a tela que contém o erro. Os erros são destacados como mostrado na figura a seguir.

2.2.7 Mostrar Uso

As mudanças feitas nos componentes de política compartilhados afetarão todas as políticas às quais estão associados. Antes de atualizar ou mudar de alguma maneira um componente de política, execute o comando *Mostrar Uso* para determinar quais políticas serão afetadas pela mudança.

1 Clique o botão direito do mouse no componente e, em seguida, clique em *Mostrar Uso*.

É exibida uma janela pop-up mostrando cada instância desse componente em outras políticas.

2.3 Importando e exportando políticas

As seções a seguir contêm mais informações:

2.3.1 Importando políticas

É possível importar uma política de qualquer localização de arquivo situada na rede disponível.

1. No Console de Gerenciamento, clique em *Arquivo* > *Importar Política*.

   Se você estiver editando ou criando uma política, o editor fechará a política (avisando que você deve gravá-la) antes de abrir a janela Importar.
2. Procure a localização do arquivo e especifique o nome de arquivo no campo.

Depois que a política for importada, ela poderá ser editada ou publicada imediatamente.

2.3.2 Exportando políticas

As políticas podem ser exportadas do Console de Gerenciamento e distribuídas por e-mail ou por um compartilhamento de rede. Esse recurso pode ser usado para distribuir políticas de nível empresarial em ambientes onde existam vários Serviços de Gerenciamento e Editores de Política distribuídos.

Para exportar uma política de segurança:

1. No Console de Gerenciamento, clique em *Arquivo* > *Exportar*.
2. Especifique um destino e dê um nome para a política com a extensão `.sen` (por exemplo, `C:\Desktop\salespolicy.sen`). Clique no botão de procura para procurar uma localização.
3. Clique em *Exportar*.

Dois arquivos são exportados. O primeiro arquivo é a política (arquivo `*.sen`). O segundo é o arquivo `setup.sen`, necessário para decodificar a política na importação.

As políticas exportadas devem ser importadas para um Console de Gerenciamento antes de serem publicadas para usuários gerenciados.

2.3.3 Exportando políticas para usuários não gerenciados

Se ZENworks Security Clients não gerenciados forem distribuídos no empreendimento, um Console de Gerenciamento Independente deverá ser instalado para a criação de políticas. Consulte o "Guia de Instalação do ZENworks Endpoint Security Management" para obter mais informações.

Para distribuir políticas não gerenciadas:

1. Localize e copie o arquivo `setup.sen` do Console de Gerenciamento para uma pasta separada.

O arquivo setup.sen é gerado na instalação do Console de Gerenciamento e é colocado no diretório \Arquivos de Programas\Novell\Console de Gerenciamento do ESM\.

2 Crie uma política no Console de Gerenciamento. Para obter mais informações, consulte Seção 2.2, “Criando políticas de segurança” na página 47.

3 Use o comando *Export* para exportar a política para a mesma pasta que contém o arquivo setup.sen.

   Todas as políticas distribuídas devem ser denominadas policy.sen para que o ZENworks Security Client as aceite.

4 Distribua os arquivos policy.sen e setup.sen. Esses arquivos devem ser copiados para o diretório \Arquivos de Programa\Novell\ZENworks Security Client\ de todos os clientes não gerenciados.

O arquivo setup.sen deve ser copiado para ZENworks Security Clients não gerenciados apenas uma vez com a primeira política. Posteriormente, apenas novas políticas devem ser distribuídas.